University of St Andrews
MMath Honours Project

Mathieu Groups M_{11} & M_{12}

- Steiner System Construction -

Emily Holmes
160001528
Supervisor: Professor Colva Roney-Dougal

Contents

Acknowledgments

I would like to thank my parents, Andy Holmes and Nathalie Holmes, for their continued support, not only during this project but throughout all my academic endeavours. Thank you for listening to all my maths talks, proofreading my work and for everything else you do for me.

I would also like to thank the most wonderful person I have ever met, Amy Edwards. Without you, none of this would be possible, so I will forever be grateful for you.

Finally, I would like to thank my project supervisor, Professor Colva Roney-Dougal. Thank you for your extreme patience with me and more support than I could have ever imagined. I am eternally grateful.

Abstract

In this project we construct the Mathieu Groups M_{11} and M_{12} as automorphism groups of W_{11} and W_{12}. In order to do this, we start by discussing group actions and transitivity. Then we introduce Steiner systems along with some of their key properties. These objects are discussed as we later define W_{11} and W_{12} to be certain Steiner systems, namely $S(4, 5, 11)$ and $S(5, 6, 12)$ respectively. We then define affine planes, a special type of Steiner system, and prove several of their properties. We do this as one of the Steiner systems we use to construct W_{11} and then W_{12} is an affine plane, called $AG_2(3)$. We then prove that $AG_2(3)$ is indeed a Steiner system and that it is unique up to isomorphism. This is needed in order to extend $AG_2(3)$ from an $S(2, 3, 9)$ Steiner system to an $S(3, 4, 10)$ which is then extended to an $S(4, 5, 11)$ Steiner system, W_{11}, and finally to an $S(5, 6, 12)$ Steiner system, W_{12}. From this we define $M_{11} := \mathrm{Aut}(W_{11})$ and $M_{12} := \mathrm{Aut}(W_{12})$. Certain properties are then proved about M_{11} and M_{12}.

The assumed knowledge of this project is covered in modules MT4516, MT4003, MT3501, MT2504 and MT2501 of the University of St Andrews.

Declaration

I certify that this project report has been written by me, is a record of work carried out by me, and is essentially different from work undertaken for any other purpose or assessment.

1 Chapter 1 - Introduction

1.1 Motivation

For many years mathematicians have tried to determine all finite simple groups. The theorem classifying the finite simple groups was proved in the 1980s [1]. The Classification Theorem is as follows [11]:

Theorem 1.1. *Let G be a finite simple group. Then G is either:*

(i) *a cyclic group of prime order;*

(ii) *an alternating group of degree $n \geq 5$;*

(iii) *a finite simple group of Lie type; or*

(iv) *one of 26 sporadic finite simple groups.*

Five of the sporadic groups were discovered by Emile Mathieu in the 1860s and the other 21 were found between 1965 and 1975. The groups Emile Mathieu introduced are called the Mathieu groups and are denoted $M_{11}, M_{12}, M_{22}, M_{23}$ and M_{24} [12].

As these groups do not fit into an infinite family of finite simple groups we must construct them. We can do this by defining these groups as the automorphism groups of certain Steiner systems as done in [3].

The two smallest of the Mathieu groups are M_{11} and M_{12}. We shall show in Chapter 5 that:

- $M_{11} = \mathrm{Aut}(S(4, 5, 11))$;
- $M_{12} = \mathrm{Aut}(S(5, 6, 12))$.

This means that we must look into Steiner systems in order to understand the Mathieu groups. We shall also prove that:

- $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8$;
- $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

We can also prove other properties of M_{11} and M_{12}, such as the fact that they are both multiply-transitive, a term we will define later. In order to show this though, we must first look into transitivity and therefore group actions. All of the properties of M_{11} and M_{12} stated here can be found in [3].

1.2 Main focus of Project

I have focused on M_{11} and M_{12} and their constructions by following the proofs in [3]. The bulk of this project focuses on the construction of the Steiner systems which are needed to construct M_{11} and M_{12}. These Steiner systems are $S(2,3,9)$, $S(3,4,10)$, $S(4,5,11)$ and $S(5,6,12)$. The aim is to construct these Steiner systems, show that they are unique up to isomorphism and then prove certain properties of their automorphism groups.

1.3 Outline of Project

We will now discuss the outline of each chapter and therefore the outline of the project.

In Chapter 2 we define group actions and prove several important theorems from group theory, such as the orbit stabiliser property. We also define transitivity and multiple-transitivity along with proving certain properties of multiply-transitive groups. Examples are given throughout.

In Chapter 3 we introduce Steiner systems and discuss their properties. We also prove key properties of automorphisms of Steiner systems. These are crucial to our constructions of M_{11} and M_{12} as these groups are automorphism groups of Steiner systems. Furthermore we define a special type of Steiner system called an affine plane. We prove certain properties of affine planes that will be useful to us in our proofs of uniqueness of certain Steiner systems.

In Chapter 4 we give some definitions and theorems regarding affine groups. Then we move onto the affine plane $AG_2(3)$. We prove several properties of this plane, including theorems about geometric figures $AG_2(3)$ contains. We shall also state and prove certain properties of the automorphism group of $AG_2(3)$. We then move onto the first big theorem of the project: $AG_2(3)$ is an $S(2,3,9)$ Steiner system and is unique up to isomorphism. After we have done this, we extend $AG_2(3)$ to an $S(3,4,10)$ Steiner system by adding a point along with appropriate blocks. Then we prove that this new Steiner system is unique up to isomorphism and call it W_{10}. Finally, some properties of $\mathrm{Aut}(W_{10})$ will be proved.

In Chapter 5 we first construct the one-point extension of W_{10} and prove that it is unique. We do this by proving that, if such an $S(4,5,11)$ Steiner system exists, then it is unique due to the uniqueness of W_{10}. Then we construct this unique Steiner system and call it W_{11}. We define $M_{11} := \mathrm{Aut}(W_{11})$ and prove some properties of M_{11}. We then construct the one-point extension of W_{11} and prove that it is unique in a very similar way. We define $M_{12} := \mathrm{Aut}(W_{12})$ and prove some properties of M_{12}. We then finish with a short conclusion about what we have achieved and what we would have looked at given more time.

2 Chapter 2

2.1 Group Actions

The following subsection introduces group actions, permutation representations and various properties of certain actions. These definitions, along with some of the examples, are taken from a combination of [3], [4], [6], [7] and [8]. First however we start with the concept of a symmetry.

Given a structured object of any sort, a *symmetry* is a bijection of the object onto itself which preserves the structure. Equivalently, a *symmetry* is a bijection from a set Ω to itself with a distance function which preserves the distance between each pair of points (i.e. an isometry).

In a visual sense, we can move the object around as much as we like as long as it 'looks' the same at the end, and the 'things' that were next to each other before the move, are still next to each other.

Example 2.1. One of the symmetries of the octahedral graph, shown in Figure 1, is the 'rotation' where vertex 1 goes to 2, 2 to 3 and so on. Another symmetry of this graph is the 'reflection' where vertex 1 goes to 2, 6 to 3 and 5 to 4 as well as vice versa.

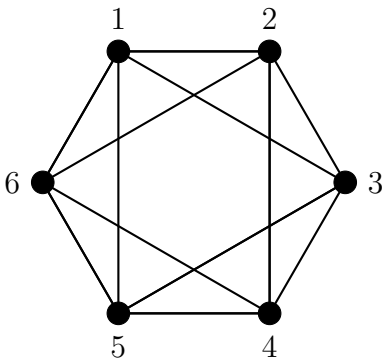

Figure 1: The octahedral graph

Definition 2.2. Let G be a group and Ω be a nonempty set, and suppose for each $\alpha \in \Omega$ and each $x \in G$ we have defined an element of Ω denoted by α^x (in other words, $(\alpha, x) \mapsto \alpha^x$ is a function from $\Omega \times G$ into Ω).
Then we say that this defines an *action* on G on Ω (or G *acts* on Ω) if we have:

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$ (where 1 denotes the identity element of G); and

(ii) $(\alpha^x)^y = \alpha^{(xy)}$ for all $\alpha \in \Omega$ and all $x, y \in G$.

Example 2.3. Let Ω be a nonempty set and let G be a subgroup of $Sym(\Omega)$. Then G acts on Ω by letting α^x be the image of α under the permutation x. Condition (i) in the definition above is satisfied by the definition of the identity element of $Sym(\Omega)$ and condition (ii) is satisfied by the definition of composition of maps. This action is called the *natural action* of G on Ω and we shall assume that this is is the action we are dealing with whenever we have a group of permutations unless explicitly stated otherwise.

Example 2.4. The group of symmetries of the octahedral graph, Figure 1, acts on both the set of 6 vertices and the set of 12 edges. The identity map is a symmetry and does not move any of the vertices, hence (i) is satisfied, also symmetries are maps and so (ii) is satisfied by the composition of maps.

Theorem 2.5. *Let a group G act on a non-empty set Ω.*
Then to each element $x \in G$ there corresponds a mapping $\overline{x}$ of Ω into itself, defined by $\overline{x} : \alpha \mapsto \alpha^x$. The mapping $\bar{x}$ is a permutation. Moreover, the map $\rho : G \to Sym(\Omega)$ defined by $\rho : x \mapsto \overline{x}$ is a homomorphism.

Proof. This proof follows that of [8].

Let $x \in G$. By definition, $\overline{x}$ is a map of Ω into itself. Use $\cdot$ to represent the composition of maps. For $x, y \in G$ and $\alpha \in \Omega$, using Definition 2.2 (ii) we have

$$\begin{aligned} \alpha(\overline{xy}) = \alpha^{xy} = (\alpha^x)^y = \alpha(\overline{x} \cdot \overline{y}), \\ \text{so} \quad \overline{xy} = \overline{x} \cdot \overline{y}. \end{aligned}$$

Moreover, using (i) from Definition 2.2 we have

$$\begin{aligned} \alpha(\overline{1_G}) = \alpha^{1_G} = \alpha \quad \text{for all } \alpha \in \Omega, \\ \text{so} \quad \overline{1_G} = 1_{Sym(\Omega)}. \end{aligned}$$

Using both of these facts

$$\begin{aligned} \overline{x} \cdot \overline{x^{-1}} = \overline{xx^{-1}} = \overline{1_G} = 1_{Sym(\Omega)}, \\ \text{and hence} \quad \overline{x} \cdot \overline{x^{-1}} = 1 = \overline{x^{-1}} \cdot \overline{x}. \end{aligned}$$

Therefore $\overline{x}$ has inverse $\overline{x^{-1}}$, so is a bijection from Ω to itself, which means $\overline{x}$ is a permutation of Ω. Also,

$$\rho(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \rho(x)\rho(y).$$

So ρ is a homomorphism of G into $Sym(\Omega)$. □

Definition 2.6. A homomorphism from G to $\mathrm{Sym}(\Omega)$ is called a (*permutation*) *representation* of G on Ω.

Definition 2.7. We say that the map ρ in Theorem 2.5 is the *permutation representation* of G *corresponding to the action* of G on Ω in Theorem 2.5.

Hence we see that each action of G on Ω gives rise to a representation of G on Ω. Conversely, we now will prove that representations also correspond to actions.

Lemma 2.8. *Let $\rho : G \to Sym(\Omega)$ be a representation of the group G on the set Ω. Then there exists an action of G on Ω defined by $\alpha^x := \alpha^{\rho(x)}$ for all $\alpha \in \Omega$ and $x \in G$. The homomorphism ρ is the representation which corresponds to this action.*

Proof. This proof follows that of [8].

First we must check that the mapping defined by $\alpha^x := \alpha^{\rho(x)}$ is in fact an action of G on Ω. We define $\cdot$ to be the binary operation in G.

(i) Let $\alpha \in \Omega$ and $x \in G$.
Then by the definition of the action

$$\alpha^1 = \alpha^{\rho(1)}.$$

The map ρ is a homomorphism so

$$\rho(1) = 1_{Sym(\Omega)}.$$

Therefore

$$\alpha^1 = \alpha^{\rho(1)} = \alpha^{1_{Sym(\Omega)}} = \alpha \quad \forall \alpha \in \Omega.$$

(ii) Let $\alpha \in \Omega$ and $x, y \in G$. Then

$$\begin{aligned}(\alpha^x)^y &= (\alpha^{\rho(x)})^{\rho(y)} \\ &= \alpha^{\rho(x)\rho(y)} \quad \text{(by the composition of maps)} \\ &= \alpha^{\rho(xy)} \quad \text{(as } \rho \text{ is a homomorphism)} \\ &= \alpha^{xy}.\end{aligned}$$

So we have proved that the mapping defined by $\alpha^x := \alpha^{\rho(x)}$ is in fact an action of G on Ω. Now we will prove that ρ is the representation which corresponds to this action.

Let $\alpha \in \Omega$ and $x \in G$.
We define $\overline{x}$ as before to be $\bar{x} : \alpha \mapsto \alpha^x$, so that $\overline{x} \in Sym(\Omega)$.

Now we define a mapping $\rho_1 : G \to Sym(\Omega)$ to be $\rho_1(x) := \overline{x}$.
By definition this map is the representation which corresponds to the action defined in the statement. So

$$\begin{aligned} \alpha^{\rho_1(x)} &= \alpha^{\overline{x}} && \text{(by the definition of } \rho_1) \\ &= \alpha^{x} && \text{(by the definition of } \overline{x}) \\ &= \alpha^{\rho(x)} && \text{(by the definition of the action in the statement).} \end{aligned}$$

Therefore ρ is equal to ρ_1 as they map elements of Ω to the same elements and they do this for every element of Ω. This means that ρ is the representation which corresponds to the group action described in the statement. □

Representations correspond to actions and vice versa. This means that we can think of group actions and permutation representations as different ways of describing the same thing.

Definition 2.9.

- The *degree* of an action (or representation) on Ω is the size of Ω.
- The *kernel* of an action is the kernel ($\ker\rho$) of the corresponding representation ρ.
- An action is *faithful* when $\ker\rho = 1$.

Corollary 2.10. *If an action ρ is faithful, then Im ρ is isomorphic to G.*

Proof. ρ is a representation and so is a homomorphism from G to Sym(Ω), therefore by the first isomorphism theorem, G / ker $\rho \cong$ Im ρ. But ρ is faithful so ker $\rho = 1$, which means that Im $\rho \cong G/1 \cong G$. □

Definition 2.11. When a group G acts on a set Ω, a typical point α is moved by elements of G to various other points of Ω. The set of these images is called the *orbit* of α under G, and we denote it by

$$\alpha^G := \{\alpha^x \mid x \in G\}.$$

Definition 2.12. The set of elements of G which fix a specified point $\alpha \in \Omega$ is called the *stabiliser* of α in G and is denoted

$$G_\alpha := \{x \in G \mid \alpha^x = \alpha\}.$$

Theorem 2.13. *Let G be a group, acting on a set Ω, and let $x, y \in G$ and $\alpha, \beta \in \Omega$. Then:*

(i) *Two orbits α^G and β^G are either equal (as sets) or disjoint, so the set of all orbits is a partition of Ω into mutually disjoint subsets.*

(ii) *The stabiliser G_α is a subgroup of G and $G_\beta = x^{-1}G_\alpha x$ whenever $\beta = \alpha^x$. Moreover, $\alpha^x = \alpha^y$ if and only if $G_\alpha x = G_\alpha y$.*

(iii) *(The orbit-stabiliser property) $|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, if G is finite then $|\alpha^G||G_\alpha| = |G|$.*

Proof. This proof follows that of [3].

(i) Let $\delta \in \alpha^G$. This means that $\delta = \alpha^g$ for some $g \in G$. Let $x \in G$. If x runs over the whole group of G then so does gx. As otherwise $gx_1 = gx_2$ for some $x_1 \neq x_2$ and $x_1, x_2 \in G$, but $g^{-1}gx_1 = g^{-1}gx_2 \implies x_1 = x_2$. From this we get a contradiction. So $\delta^G = \{\delta^x \mid x \in G\} = \{\alpha^{gx} \mid x \in G\} = \alpha^G$. If $\delta \in \beta^G$ as well (i.e. α^G and β^G have an element in common) then $\beta^G = \delta^G = \alpha^G$. Every element $\alpha \in \Omega$ lies in at least one orbit, and we have shown here that it cannot lie in more than one orbit, so the set of all orbits partitions Ω.

(ii) We know that $\alpha^1 = \alpha$, so $1 \in G_\alpha$. And if $x, y \in G_\alpha$, $\alpha = \alpha^x = \alpha^y$, so $\alpha^{xy^{-1}} = \alpha$, which means that $xy^{-1} \in G_\alpha$. This shows that G_α is a subgroup of G.

If $\beta = \alpha^x$, then:

$$y \in G_\beta \iff \beta^y = \beta \iff \alpha^{xy} = \alpha^x \iff \alpha^{xyx^{-1}} = \alpha \iff xyx^{-1} \in G_\alpha.$$

This is true for all $y \in G_\beta$, so $xG_\beta x^{-1} = G_\alpha$, which implies $G_\beta = x^{-1}G_\alpha x$.

Finally,

$$\alpha^x = \alpha^y \iff \alpha^{xy^{-1}} = \alpha \iff xy^{-1} \in G_\alpha \iff G_\alpha xy^{-1} = G_\alpha \iff G_\alpha x = G_\alpha y.$$

(iii) By (ii), the distinct points in α^G are in bijective correspondence with the right cosets of G_α in G. To get the case for when G is finite, we use Lagrange's theorem.

□

2.2 Transitivity

This subsection introduces transitivity using definitions and theorems from [3]. We then move onto k-transitivity and sharp k-transitivity. We prove several theorems about groups with these properties as this will help us demonstrate properties of M_{11} and M_{12}. These theorems are taken from [3] and [9].

Definition 2.14. A group G acting on a set Ω is said to be *transitive* on Ω if it has only one orbit, and so $\alpha^G = \Omega$ for all $\alpha \in \Omega$.

Equivalently, G is *transitive* if for every pair of points $\alpha, \beta \in \Omega$, there exists $x \in G$ such that $\alpha^x = \beta$.

A group which is not transitive is called *intransitive*.

Definition 2.15. A group acting transitively on a set Ω is said to be acting *regularly* if $G_\alpha = 1$ for each $\alpha \in \Omega$. Only the identity fixes any point.

Corollary 2.16. *Let G act transitively on a set Ω. Then:*

(i) *The stabilisers G_α ($\alpha \in \Omega$) form a single conjugacy class of subgroups of G;*

(ii) *The index $|G : G_\alpha| = |\Omega|$ for each α;*

(iii) *If G is finite then the action of G is regular if and only if $|G| = |\Omega|$.*

Proof. (i) Let $\alpha, \beta \in G$, then there exists a $x \in G$ such that $\alpha^x = \beta$ as G is transitive. By Theorem 2.13(ii) $G_\beta = x^{-1}G_\alpha x$ so G_α and G_β are conjugate and so in the same conjugacy class. Our choices of α and β were arbitrary and so this is true for all stabilisers of points in G.

(ii) Let $\alpha \in G$, then $|G : G_\alpha| = |\alpha^G|$ by Theorem 2.13(iii) and as G is transitive $\alpha^G = \Omega$, so $|G : G_\alpha| = |\Omega|$

(iii) Let $\alpha \in G$. G is finite, so by (ii) and Lagrange's Theorem

$$|\Omega| = |G : G_\alpha| = |G||G_\alpha| = |G|$$

as $|G_\alpha| = 1$.

□

Example 2.17. We illustrate these concepts by calculating the order of the group G of symmetries of the octahedral graph. This is an adaptation of an example in [3]. Consider the action of the group G on the set Ω of vertices as in Figure 1. Let $x, y \in G$ such that the corresponding permutations $\overline{x}$ and $\overline{y}$ induce on Ω are (135)(246) and (14)(25)(36) respectively. These maps clearly send edges to edges and non-edges to non-edges. The subgroup generated by x, $\langle x \rangle$, has orbits {1,3,5} and {2,4,6} and, similarly $\langle y \rangle$ has orbits {1,4}, {2,5}, {3,6}. The vertex 1 can be mapped to any other vertex using only xs and ys, therefore the orbit of 1 under $\langle x, y \rangle$ is Ω. This means that $\langle x, y \rangle$ is transitive on Ω. So for every pair of points $\alpha, \beta \in \Omega$, there exists a combination of xs and ys, call it g, such that $\alpha^g = \beta$. Since $x, y \in G$, G is transitive. By the orbit-stabiliser property, $|G : G_1| = |1^G| = |\Omega| = 6$.

Next we consider the action of the subgroup G_1. Any symmetry of the graph which fixes vertex 1 must also fix the unique non-neighbour of 1, vertex 4, and map the vertices 2 and 6 amongst themselves because they are the only common neighbours of 1 and 4. The element $z \in G$ which maps $2 \leftrightarrow 6$ and $3 \leftrightarrow 5$ induces the permutation $\overline{z} = (1)(26)(35)(4) = (26)(35)$ on Ω and lies in G_1 as it does not move 1. So $\{2, 6\}$ is an orbit for G_1 as neither of them can be mapped to any other element of Ω by an element of G_1 but they can be mapped to one another. Thus the stabiliser G_{12} of 2 in G_1 satisfies $|G_1 : G_{12}| = |2^G| = 2$.

Finally, we consider the stabiliser of two points G_{12}. Each symmetry which fixes 1 and 2 must also fix 5 and 4. We can however swap 3 and 6 as they are both adjacent to all four of $\{1, 2, 4, 5\}$. So $|G_{12}| = 2$ as it contains identity map and the permutation (36). Thus we conclude that

$$|G| = |G : G_1||G_1 : G_{12}||G_{12}| = 6 \cdot 2 \cdot 2 = 24.$$

Definition 2.18. Let G be a group acting on a set Ω and k be an integer such that $1 \leq k \leq |\Omega|$. We say that G is *k-transitive* if G is transitive on the set of k-tuples of distinct points, which we call $\Omega^{(k)}$.

Theorem 2.19. $|\Omega^{(k)}| = |\Omega||\Omega - 1| \dots |\Omega - (k-1)|$.

Proof. There are $|\Omega|$ choices for the first point, $|\Omega - 1|$ for the second and so on until there are $|\Omega - (k-1)|$ choices for the k-th and final point. □

The following Lemma is Exercise 2.1.1 of [3]

Lemma 2.20. *Let G be a group acting on Ω. G is transitive if and only if G is 1-transitive on Ω. Moreover, if $k > 1$, then G is $(k-1)$-transitive on Ω whenever G is k-transitive on Ω.*

Proof. Let G be a group acting on Ω.

$$\begin{aligned} G \text{ transitive on } \Omega &\iff \forall\ \alpha, \beta \in \Omega,\ \exists\ x \in G \text{ such that } \alpha^x = \beta \\ &\iff \forall\ (\alpha), (\beta) \in \Omega^{(1)},\ \exists\ x \in G \text{ such that } (\alpha)^x = (\alpha^x) = \beta \\ &\iff G \text{ is 1-transitive.} \end{aligned}$$

So we have proved the first part.

Now, assume G is k-transitive. This means that

$$\begin{aligned} &\forall\ (\alpha_1, \alpha_2, \dots, \alpha_k), (\beta_1, \beta_2, \dots, \beta_k) \in \Omega^{(k)}, \\ &\exists\ x \in G \text{ such that } (\alpha_1, \alpha_2, \dots, \alpha_k)^x = (\alpha_1^x, \alpha_2^x, \dots, \alpha_k^x) \\ &\qquad\qquad = (\beta_1, \beta_2, \dots, \beta_k). \end{aligned}$$

Let $(\delta_1, \delta_2, \ldots, \delta_{k-1}), (\gamma_1, \gamma_2, \ldots, \gamma_{k-1}) \in \Omega^{(k-1)}$.

From the definition of $\Omega^{(k)}$ we know that the α_i for $1 \leq i \leq k$ are all distinct. This mean that $|\Omega| \geq k$. So we know there exists an $\alpha \in \Omega \backslash \{\delta_1, \ldots \delta_{k-1}\}$ and a $\beta \in \Omega \backslash \{\gamma_1, \ldots \gamma_{k-1}\}$. Therefore $(\delta_1, \ldots, \delta_{k-1}, \alpha), (\gamma_1, \ldots, \gamma_{k-1}, \beta) \in \Omega^{(k)}$.

As G is k-transitive we know that there exists an $x \in G$ such that $(\delta_1, \ldots, \delta_{k-1}, \alpha)^x = (\gamma_1, \ldots, \gamma_{k-1}, \beta)$.

This means that $\delta_i^x = \gamma_i$ for $1 \leq i \leq k-1$. So

$$\begin{aligned}(\gamma_1, \gamma_2, \ldots, \gamma_{k-1}) &= (\delta_1^x, \delta_2^x, \ldots, \delta_{k-1}^x) \\ &= (\delta_1, \delta_2, \ldots, \delta_{k-1})^x.\end{aligned}$$

Therefore G is $(k-1)$-transitive. □

Theorem 2.21. *Let a group G act i-transitively on a set Ω and $(\alpha_1, \ldots, \alpha_i) \in \Omega^{(i)}$. If the stabiliser $G_{(\alpha_1, \ldots, \alpha_i)}$ acts $(k-i)$-transitively on $\Omega \backslash \{\alpha_1, \ldots, \alpha_i\}$, where $k-i+1 \geq 2$, then G acts k-transitively on Ω.*

Proof. This proof is an extension of the proof in [9].

Let $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k) \in \Omega^{(k)}$. We want to show that there exists $f \in G$ such that $(y_1, \ldots, y_k)^f = (x_1, \ldots, x_k)$.

Let $(\alpha_1, \ldots, \alpha_i) := (x_{k-i+1}, \ldots, x_k)$. This means that $x_1, \ldots, x_{k-i}$ are distinct elements in $\Omega \backslash \{\alpha_1, \ldots, \alpha_i\}$. As G acts i-transitively on Ω, there exists $g \in G$ such that $(\alpha_1, \ldots, \alpha_i)^g = (y_{k-i+1}, \ldots, y_k)$. Let ${y_i}^g = z_i$ where $1 \leq i \leq k-i$. Therefore $(y_1, \ldots, y_{k-i}, y_{k-i+1}, \ldots, y_k)^g = (z_1, \ldots, z_{k-i}, \alpha_1, \ldots, \alpha_i)$. Since $G_{(\alpha_1, \ldots, \alpha_i)}$ is $(k-i)$-transitive on $\Omega \backslash \{\alpha_1, \ldots, \alpha_i\}$, there exists an element $h \in G_{(\alpha_1, \ldots, \alpha_i)}$ such that $(z_1, \ldots, z_{k-i})^h = (x_1, \ldots, x_{k-i})$. This means that

$$\begin{aligned}(y_1, \ldots, y_{k-i}, y_{k-i+1}, \ldots, y_k)^{gh} = (z_1, \ldots, z_{k-i}, \alpha_1, \ldots, \alpha_i)^h &= (x_1, \ldots, x_{k-i}, \alpha_1, \ldots, \alpha_i) \\ &= (x_1, \ldots, x_{k-i}, x_{k-i+1}, \ldots, x_k).\end{aligned}$$

Therefore $f = gh$. □

Corollary 2.22. *Let a group G act transitively on a set Ω and $\alpha \in \Omega$. If the stabiliser G_α acts $(k-1)$-transitively on $\Omega \backslash \{\alpha\}$, where $k \geq 2$, then G acts k-transitively on Ω.*

Proof. Let $i = 1$ in Theorem 2.21. □

Definition 2.23. Let G be a group acting on a set Ω. Then G is *sharply k-transitive* if for every pair of elements in $\Omega^{(k)}$, $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$, there exists a unique $x \in G$ such that $(\alpha_1, \ldots, \alpha_k)^x = (\beta_1, \ldots, \beta_k)$.

The following Theorem is left as an exercise for the reader in [9].

Theorem 2.24. *Let a group G acting on a set Ω. Then G is sharply k-transitive on Ω if and only if G is k-transitive and the stabiliser of any k-tuple of distinct points in Ω is the identity.*

Proof. We first assume that G is sharply k-transitive on Ω. Therefore for every $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k) \in \Omega^{(k)}$, there exists a unique $g \in G$ such that $(x_1, \ldots, x_k)^g = (y_1, \ldots, y_k)$. It is clear from this that G is k-transitive on Ω. Now if we assume by way of contradiction that there exists a non-identity element in $G_{(x_1,\ldots,x_k)}$, say f, then $(x_1, \ldots, x_k)^f = (x_1, \ldots, x_k)$ and so $(x_1, \ldots, x_k)^{fg} = (y_1, \ldots, y_k)$. The only way to get $fg = g$ is if $f = 1$. Therefore we get a contradiction.

Now we assume that G is k-transitive on Ω and the stabiliser of any k-tuple of distinct points in Ω is the identity. We assume by way of contraction that G is not sharply k-transitive on Ω. From this and the assumption that G is k-transitive, we know that there exists 2 distinct elements of G that map $(x_1, \ldots, x_k)$ to $(y_1, \ldots, y_k)$ where $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in \Omega^{(k)}$. We call these 2 elements in G, g and h. Therefore

$$(x_1, \ldots, x_k)^g = (y_1, \ldots, y_k) \text{ and } (x_1, \ldots, x_k)^h = (y_1, \ldots, y_k).$$

So

$$(x_1, \ldots, x_k)^{gh^{-1}} = (x_1, \ldots, x_k).$$

But we have assumed that the only element in G which fixes $(x_1, \ldots, x_k)$ is the identity, therefore $gh^{-1} = 1$. This forces $g = h$, which is a contradiction. □

Theorem 2.25. *Let G be a group which acts on a set Ω. If G has size $|\Omega^{(k)}|$ and $|G_{(x_1,\ldots,x_k)}| = 1$ for each $(x_1, \ldots, x_k) \in \Omega^{(k)}$, then G is sharply k-transitive on Ω.*

Proof. We have assumed that $|G_{(x_1,\ldots,x_k)}| = 1$ and $|G| = |\Omega^{(k)}|$. This means that

$$|(x_1, \ldots, x_k)^G| = |G|/|G_{(x_1,\ldots,x_k)}| = |\Omega^{(k)}|.$$

Therefore G is k-transitive on Ω.

Also because we have assumed that the stabiliser of any k-tuple of distinct points in Ω is the identity, we can use Theorem 2.24. Therefore G is sharply k-transitive on Ω. □

Theorem 2.26. *Let a group G act i-transitively on a set Ω and let $G_{(x_1,\ldots,x_{k-i})}$ act sharply $(k-i)$-transitively on $\Omega \backslash \{x_1, \ldots, x_{k-i}\}$. Then G acts sharply k-transitive on Ω.*

Proof. As $G_{(x_1,\ldots,x_{k-i})}$ acts sharply $(k-i)$-transitively on $\Omega\backslash\{x_1,\ldots,x_{k-i}\}$, the stabiliser of any $(k-i)$-tuples of distinct points in $\Omega\backslash\{x_1,\ldots,x_{k-i}\}$ is the identity by Theorem 2.24. Also by Theorem 2.21, the group G is k-transitive on Ω.

If the stabiliser of any k-tuples of distinct points in Ω is the identity then G acts sharply k-transitive on Ω by Theorem 2.24 and the fact that G is k-transitive on Ω.

We assume by way of contradiction that there exists a $g \in G\backslash\{1_G\}$ such that $(x_1,\ldots,x_i,\ldots,x_k)^g = (x_1,\ldots,x_i,\ldots,x_k)$ where $(x_1,\ldots,x_i,\ldots,x_k) \in \Omega^{(k)}$. This means that

$$(x_1,\ldots,x_i)^g = (x_1,\ldots,x_i) \implies g \in G_{(x_1,\ldots,x_i)}.$$

But $x_{i+1},\ldots,x_k$ are $k-i$ distinct points in $\Omega\backslash\{x_1,\ldots,x_i\}$ and

$$(x_{i+1},\ldots,x_k)^g = (x_{i+1},\ldots,x_k).$$

This forces g to be the identity in G as the stabiliser of any $(k-i)$-tuples of distinct points in $\Omega\backslash\{x_1,\ldots,x_{k-i}\}$ is the identity. So we get a contradiction. Therefore G acts sharply k-transitive on Ω as stabiliser of any k-tuples of distinct points in Ω is the identity. □

Theorem 2.27. *Let G act k-transitively on a set Ω. Then*

$$|G| = n(n-1)\ldots(n-k+1)|G_{(x_1,\ldots,x_k)}|,$$

where $|\Omega| = n$ and $(x_1,\ldots,x_k) \in \Omega^{(k)}$.

Proof. This proof follows that of [9].

As G act k-transitively on a set Ω, then by repetitive use of Lemma 2.20, we can see that G acts transitively on Ω. Therefore by the orbit stabiliser property

$$|G| = |x_1^G||G_{x_1}| = n|G_{x_1}|.$$

Since G acts k-transitively, G_{x_1} acts $(k-1)$-transitively on $\Omega\backslash\{x_1\}$. Once again by repetitive use of Lemma 2.20, we can see that G_{x_1} acts transitively on $\Omega\backslash\{x_1\}$. Therefore by the orbit stabiliser property

$$|G_{x_1}| = |x_2^{G_{x_1}}||G_{(x_1,x_2)}| = (n-1)|G_{(x_1,x_2)}|.$$

If we continue to use this logic we see that for $i \leq k$

$$|G_{x_{i-1}}| = |x_i^{G_{x_{i-1}}}||G_{(x_1,\ldots,x_i)}| = (n-i)|G_{(x_1,\ldots,x_i)}|.$$

Therefore

$$|G| = n(n-1)\ldots(n-k+1)|G_{(x_1,\ldots,x_k)}|.$$

□

Corollary 2.28. *If G acts sharply k-transitively on Ω, where $|\Omega| = n$, then*

$$|G| = n(n-1)\dots(n-k+1).$$

Proof. As G acts sharply k-transitively on Ω, then $|G_{(x_1,\dots,x_k)}| = 1$ for any $(x_1,\dots,x_k) \in \Omega^{(k)}$ by Theorem 2.24. Therefore by Theorem 2.27

$$|G| = n(n-1)\dots(n-k+1)|G_{(x_1,\dots,x_k)}| = n(n-1)\dots(n-k+1).$$

□

3 Chapter 3

3.1 Steiner Systems

In this subsection we introduce the concept of Steiner systems and prove various properties of these objects. Most of these definitions and theorems are taken from [3]. It is crucial that we study Steiner systems and their properties as we are later going to construct M_{11} and M_{12} as automorphism groups of certain Steiner systems.

Definition 3.1. An $S(t, k, v)$ *Steiner system* $S = S(\Omega, \mathcal{B})$ is a finite set Ω of v *points* together with a set $\mathcal{B}$ of subsets called *blocks* each of size k such that any t points of Ω lies in exactly one block from $\mathcal{B}$.

The parameters are assumed to satisfy $0 < t < k < v$ to eliminate trivial examples. We also define another parameter b to be the number of blocks in a given Steiner system, i.e. $b = |\mathcal{B}|$.

An automorphism of a Steiner system $S(\Omega, \mathcal{B})$ is a permutation on the point of Ω such that the blocks are permuted among themselves.

Theorem 3.2. *The number r of blocks containing a given element of Ω is $\binom{v-1}{t-1}/\binom{k-1}{t-1}$.*

Proof. This proof follows that of [3].

Let $S = S(\Omega, \mathcal{B})$ be an $S = S(t, k, v)$ Steiner System and let α be an element of Ω, i.e. a point.

The way we find r is by counting the number of t-subsets (sets of size t) of Ω containing α in two different ways.

The first way to count this is simply by looking at the whole of Ω. We need $t-1$ more elements of the set from $v-1$ elements of Ω (cannot choose α again). Hence the number of t-subsets of Ω containing α is $\binom{v-1}{t-1}$.

The second way of counting this is is to look at each block which contains α. Each t-subset lies in a unique block so we will be counting every t-subset exactly once. Similar to above, every block contains $\binom{k-1}{t-1}$ t-subsets containing α. To find the total number of t-subsets of Ω containing α we must multiply this by the number of blocks which contain α, r.

Equating the two, we get

$$\binom{v-1}{t-1} = r\binom{k-1}{t-1}.$$

Therefore

$$r = \binom{v-1}{t-1}/\binom{k-1}{t-1}.$$

□

Corollary 3.3. *The number λ_i of blocks which contains a specified i-subset where $1 \leq i \leq t$ is independent of the subset chosen and is given by*

$$\lambda_i = \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = \frac{(v-i)(v-i-1)\cdots(v-t+1)}{(k-i)(k-i-1)\cdots(k-t+1)} \quad for\ i = 1, \ldots, t.$$

Notice that $\lambda_i > 0$.

Proof. Same as previous proof except we are counting t-subsets which contain a given set of size i. To amend the proof we exchange a given point α for a given set of size i, and then replace 1 with i in subsequent counting. □

Remark: v, k and t must be such that each of the expressions for λ_i is an integer.

Corollary 3.4. *Let $S = S(\Omega, \mathcal{B})$ be an $S = S(t, k, v)$ Steiner System in which each point of Ω lies in exactly r blocks. Then*

$$r = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

Proof. This follows from the calculations above as $r = \lambda_1$. □

Definition 3.5. Let $S = S(\Omega, \mathcal{B})$ be a Steiner System. An *incidence matrix* for a Steiner system is a matrix whose rows are indexed by the set Ω and whose rows are indexed by B (both Ω and B are in an arbitrary order). The (α, B)-th entry of this matrix is 1 if $\alpha \in B$ and 0 otherwise.

The following Lemma is Exercise 6.2.2 in [3].

Lemma 3.6. *An $n \times n$ matrix of the form*

$$\begin{bmatrix} a_1 + c & a_1 & \ldots & a_1 \\ a_2 & a_2 + c & \ldots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & \ldots & a_n + c \end{bmatrix}$$

has the determinant $c^{n-1}(c + a_1 + \cdots + a_n)$.

Proof. Call this matrix A. The crux of this proof lies in elementary row and column operations, namely adding a multiple of one row/column to another. These operations

do not change the determinant of the matrix. Firstly we add one of each row to the top row. The resulting matrix looks like this

$$\begin{bmatrix} a_1+a_2+\cdots+c & a_1+a_2+\cdots+c & \dots & a_1+a_2+\cdots+c \\ a_2 & a_2+c & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & \dots & a_n+c \end{bmatrix}.$$

We then take away the first column from all other columns, leaving us with

$$\begin{bmatrix} a_1+a_2+\cdots+c & 0 & \dots & 0 \\ a_2 & c & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \dots & c \end{bmatrix}.$$

Next we calculate the determinant going across the first row.

$$detA = (a_1+a_2+\cdots+c)\cdot det\begin{bmatrix} c & 0 & \dots & 0 \\ 0 & c & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & c \end{bmatrix}.$$

Note that this matrix with only c's and 0's is $n-1 \times n-1$. Multiplying a row of a matrix by a scalar multiplies the determinant by the same scalar. If we multiply each of the $n-1$ rows of this new matrix by $\frac{1}{c}$, we get the following:

$$det\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = \frac{1}{c^{n-1}}\cdot det\begin{bmatrix} c & 0 & \dots & 0 \\ 0 & c & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & c \end{bmatrix}.$$

So

$$\begin{aligned} detA &= (a_1+a_2+\cdots+c)\cdot c^{n-1}\cdot det(I_{n-1}) \\ &= c^{n-1}(c+a_1+\cdots+a_n). \end{aligned}$$

□

Lemma 3.7. *Let $S = S(\Omega, \mathcal{B})$ be an $S(t,k,v)$ Steiner system, each point of Ω lies in exactly r blocks and λ_i be as described in Corollary 3.3. Then $r > \lambda_2$.*

Proof. First we remember that the definition of λ_2 is

$$\lambda_2 = \frac{(v-2)(v-3)\cdots(v-t+1)}{(k-2)(k-3)\cdots(k-t+1)}.$$

Also we note that $v > k$ by the definition of a Steiner system, so $v-1 > k-1$. This implies

$$\frac{(v-1)}{(k-1)} > 1.$$

From this we get

$$r = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)} = \frac{(v-1)}{(k-1)} \cdot \lambda_2 > \lambda_2.$$

□

Theorem 3.8. *Let $S = S(\Omega, \mathcal{B})$ be an $S(t,k,v)$ Steiner system, S has b blocks and each point of Ω lies in exactly r blocks. Then:*

(i) *$bk = vr$;*

(ii) *(Fisher's inequality) $v \leq b$ and $k \leq r$.*

Proof. This proof follows that of [3].

(i) The way we do this is by counting the number m pairs (α, B) such that $\alpha \in B$, in two different ways. Firstly, there are b choices for B as there are b blocks. Once we have a block there are k choices for α as there are k points in each block. This means that $m = bk$. Secondly, there are v choices for α as there are v points in Ω. Once we have a point we must choose a block which contains this point. There are r choices for this block B as each point is contained in exactly r blocks. Hence $m = vr$. Putting these together gives $bk = vr$

(ii) Order the elements of Ω and $\mathcal{B}$ within themselves and then fix them. Let $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_v\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. Let A be be incidence matrix for S. Then

$$A = [a_{ij}] \quad (1 \leq i \leq v,\ 1 \leq j \leq b)$$

with

$$a_{ij} = \begin{cases} 1, & \text{if } \alpha_i \in B_j; \\ 0, & \text{otherwise.} \end{cases}$$

Now we calculate $AA^T = [b_{ij}]$ with $1 \leq i, j \leq v$.

To calculate b_{ij} we multiply the i-th row of A with the j-th column of A^T. Here we are essentially doing the dot product of the ith row of A with the jth row of A. This means we go through the b entries of the two rows at the same time, one entry at a time and multiply them together. This only affects the end result if both entries are 1 (as otherwise at least one is 0 and so the product will also be 0). This only happens when both α_i and α_j are in the same block. Therefore we are counting the number of blocks which contain both α_i and α_j.

If $i \neq j$ then this is the number of blocks which contain a specified 2-subset, and is therefore λ_2.

If $i = j$ then this is the number of blocks which contains a specified point, and is therefore r.

We conclude that

$$AA^T = \begin{bmatrix} r & \lambda_2 & \dots & \lambda_2 \\ \lambda_2 & r & \dots & \lambda_2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_2 & \lambda_2 & \dots & r \end{bmatrix} = \begin{bmatrix} \lambda_2 + (r - \lambda_2) & \lambda_2 & \dots & \lambda_2 \\ \lambda_2 & \lambda_2 + (r - \lambda_2) & \dots & \lambda_2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_2 & \lambda_2 & \dots & \lambda_2 + (r - \lambda_2) \end{bmatrix}.$$

By Lemma 3.6

$$\begin{aligned} det(AA^T) &= (r - \lambda_2)^{v-1}(r - \lambda_2 + v\lambda_2) \\ &= (r - \lambda_2)^{v-1}(r + (v - 1)\lambda_2). \end{aligned}$$

By Lemma 3.7, $r > \lambda_2$, so $r - \lambda_2 > 0$ and $r + (v-1)\lambda_2 = r - \lambda_2 + v\lambda_2 > v\lambda_2 > 0$ as both $v, \lambda_2 > 0$. This shows that $det(AA^T) \neq 0$, which means that when AA^T is in reduced row/column form, there are no all 0 rows/columns so the rank of AA^T is number of rows/columns, which is v. When multiplying two matrices together, the rank of the new matrix cannot be greater than the rank of either of the matrices in the multiplication. Therefore the $\text{rank}(A) \geq \text{rank}(AA^T) = v$. The rank of A cannot be greater than the number of columns of A, therefore $b \geq \text{rank}(A) \geq v$. So we have proved that $v \leq b$. Now if we use part (i) we get

$$bk = vr \leq br.$$

So

$$k \leq r.$$

($b \neq 0$ as $b = \frac{vr}{k}$ and $v, r, k \neq 0$).

□

Corollary 3.9. *Let $S = S(\Omega, \mathcal{B})$ be an $S(t, k, v)$ Steiner system, S has b blocks and each point of Ω lies in exactly r blocks. Then*

$$b = \binom{v}{t} / \binom{k}{t}.$$

Proof. There are two ways of looking at this. Firstly, by Theorem 3.8 and Corollary 3.4

$$\begin{aligned} b &= \frac{vr}{k} = \frac{v}{k} \cdot \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)} \\ &= \frac{(v-1)(v-2)\cdots(v-t+1)}{t!} \Big/ \frac{(k-1)(k-2)\cdots(k-t+1)}{t!} \\ &= \binom{v}{t} / \binom{k}{t}. \end{aligned}$$

The other way of looking at it is to alter the proof of Theorem 3.2 and simply count the number of t-subsets of Ω. □

The following Lemma is Exercise 6.2.3(i) in [3]

Lemma 3.10. *Let $S = S(\Omega, \mathcal{B})$ be an $S(2, k, v)$ Steiner system. If $b > v$ then $v \geq k^2$.*

Proof. We first note that for any two integers a, b, if $a < b \implies a + 1 \leq b$.

$$\begin{aligned} vr = bk > vk &\implies r > k, \\ k < r &\implies k + 1 \leq r \quad \text{(as k and r are integers)}, \\ k + 1 \leq r = \frac{v-1}{k-1}&, \\ k^2 - 1 &\leq v - 1, \\ k^2 &\leq v. \end{aligned}$$

□

Definition 3.11. Let $S = S(\Omega, \mathcal{B})$ be an $S(t, k, v)$ Steiner system. Let $\alpha \in \Omega$ and $S_\alpha = S(\Omega', \mathcal{B}')$ where $\Omega' := \Omega \backslash \alpha$ and $\mathcal{B}' := \{\mathcal{B} \backslash \{\alpha\} \mid B \in \mathcal{B} \text{ and } \alpha \in B\}$. Then S_α is a *contraction* of S.

Also, S is an *extension* of S_α.

Remark: Contractions of a Steiner system are always possible but it is rare to find an extension of a given Steiner system.

Theorem 3.12. *S_α is an $S(t-1, k-1, v-1)$ Steiner system.*

Proof. There are $v-1$ points in Ω' as we have removed α. Each set in $\mathcal{B}'$ has size $k-1$ as we are taking all the blocks from $\mathcal{B}$ which contain α and then removing α from them.

Now we prove that every $(t-1)$-subset of Ω' lies in exactly one set of $\mathcal{B}'$. First we pick any $(t-1)$-subset of Ω' and call it T. $T \cup \{\alpha\}$ is of size t and therefore lies in exactly one block B of $\mathcal{B}$. B must contain α as T contains α. This means that $B\backslash\{\alpha\} \in \mathcal{B}'$ and $T \in B\backslash\{\alpha\}$. Therefore T lies in at least one set of $\mathcal{B}'$. If T was in more than one set of $\mathcal{B}'$, say B_1 and B_2, then $T \cup \{\alpha\}$ would be a t-subset which lies in two blocks of $\mathcal{B}$, specifically $B_1 \cup \{\alpha\}$ and $B_2 \cup \{\alpha\}$. This cannot happen and therefore T lies in exactly one set of $\mathcal{B}'$. Therefore the sets of $\mathcal{B}'$ are blocks of S_α and $S_\alpha = S(\Omega', \mathcal{B}')$ is an an $S(t-1, k-1, v-1)$ Steiner system. □

3.2 Automorphims of Steiner Systems

This subsection discusses properties of automorphims groups of Steiner Systems, which is exactly what we later define M_{11} and M_{12} to be. These theorems are exercises from [3].

The following Theorem is Exercise 6.2.9 from [3].

Theorem 3.13. *Let G be an automorphism group of a Steiner system $S = S(\Omega, \mathcal{B})$ and let $\alpha \in \Omega$. Then G_α is an automorphism group of the contraction $S_\alpha = S(\Omega', \mathcal{B}')$.*

Proof. Let $g \in G_\alpha$, $B \in \mathcal{B}$ such that $\alpha \in B$.

From the definition of S_α we know that $B\backslash\{\alpha\} \in \mathcal{B}'$.

We now look at how G acts on these sets of the form $(B\backslash\{\alpha\}) \in \mathcal{B}'$.

$$G_\alpha \subseteq G \implies B^g \in \mathcal{B}; \text{ and}$$
$$\alpha \in B \implies \alpha^g \in B^g \implies \alpha \in B^g \text{ as } g \in G_\alpha.$$

Therefore $(B\backslash\{\alpha\})^g = B^g\backslash\{\alpha\}^g = B^g\backslash\{\alpha\} \in \mathcal{B}'$.

This means elements of G_α map blocks of S_α to blocks of S_α, so $G_\alpha \subseteq \mathrm{Aut}(S_\alpha)$. □

The following Theorem is Exercise 6.2.10 from [3].

Theorem 3.14. *Suppose that a Steiner system S has an extension S^* obtained by adding the point α and the new set X of blocks. A group H of automorphisms of S is also a group of automorphisms of S^* if and only if H leaves X invariant in its induced action on the subsets of the points of S.*

Proof. Let $S = S(\Omega, \mathcal{B})$, $S^* = S(\Omega \cup \{\alpha\}, \mathcal{B}^*)$ and $H \leqslant \mathrm{Aut}(S)$.
This means that $\forall B \in \mathcal{B}$ and $\forall g \in H$, $B^g \in \mathcal{B}$. Plus it means that $H \leqslant \mathrm{Sym}(\Omega)$.
We know that $\mathcal{B}^* = X \cup \{B \cup \{\alpha\} \mid B \in \mathcal{B}\}$ and that no set in X contains α.

We first make each element of H into an element of $\mathrm{Sym}(\Omega \cup \{\alpha\})$ by letting H fix α. H acts exactly on the same Ω as it did before.

Now we assume that $H \leqslant \mathrm{Aut}(S^*)$.
We assume for contradiction that $\exists\ B \in X$ and $g \in H$ such that $B^g \notin X$. The assumption that $g \in \mathrm{Aut}(S^*)$ implies that $B^g \in \mathcal{B}^*$, so $B^g = B' \cup \{\alpha\}$ for some $B' \in \mathcal{B}$.

As $g \in H$, g fixes α, which means that g^{-1} also fixes α. So

$$\begin{aligned} B^{gg^{-1}} &= (B' \cup \{\alpha\})^{g^{-1}}, \\ B &= (B')^{g^{-1}} \cup \{\alpha\} \\ &= B'' \cup \{\alpha\} \quad (B'' \in \mathcal{B} \text{ as } g^{-1} \in \mathrm{Aut}(S)) \\ &\notin X. \end{aligned}$$

From this we get a contradiction.

Now we do the other direction and assume that H leaves X invariant.
This means that $\forall B \in X$ and $\forall h \in H$, $B^h \in X$.

Also we know that $H \subseteq \mathrm{Aut}(S)$. So $\forall B' \in \mathcal{B}$ and $\forall h \in H$, $(B')^h \in \mathcal{B}$. Furthermore, $\alpha^h = \alpha \ \ \forall h \in H$. Therefore $(B' \cup \{\alpha\})^h = B'' \cup \{\alpha\}$ where $B' \in \mathcal{B}$.

As $\mathcal{B}^* = X \cup \{B \cup \{\alpha\} \mid B \in \mathcal{B}\}$ we have finished.

□

The following Theorem is Exercise 6.2.11 from [3].

Theorem 3.15. *Let S be an $S(t, k, v)$ Steiner system and S^* be an extension of S obtained by adding a new point α to each of the blocks of S and adding some new set X of blocks. Suppose S is determined uniquely (up to isomorphism) by its parameters and that any 2 possible choices for the set X are conjugate under some automorphism of S. Then the automorphism group $Aut(S^*)$ is transitive on the points of S^*.*

Proof. Let $S^* = \{\Omega, \mathcal{B}\}$ and let α and β be two points of Ω. The set S^* is an $S(t+1, k+1, v+1)$ Steiner system. The contractions of S^* obtained by deleting α and β respectively are isomorphic to S. This is because S is determined uniquely (up to isomorphism) by its parameters and the contractions of S^* obtained by deleting α and β respectively are both $S(t, k, v)$ Steiner systems so they are therefore isomorphic to S. As both of these contractions are isomorphic to S, they are therefore isomorphic

to each other. We call our two contractions of S^*_α and S^*_β and call the isomorphism which maps S^*_α to S^*_β, ϕ. We now extend ϕ to Ω by making ϕ map α to β and call this map ψ.

As ϕ is an isomorphism, it maps the blocks of S^*_α to the blocks of S^*_β. The blocks S^* containing α are constructed by adding α to each block in S^*_α and the blocks S^* containing β are constructed by adding β to each block in S^*_β. Therefore ψ maps the blocks in S^* containing α to the blocks in S^* containing β.

Let X_α be the set of blocks of S^* not containing α. Then X_α is a set of $(k+1)$-subsets of $\Omega\backslash\{\alpha\}$ such that every $(t+1)$-subset of $\Omega\backslash\{\alpha\}$ which is not contained in a block of S^*_α is in exactly one of the sets in X_α. As ϕ is an isomorphism it preserves structure. This means that X^ϕ_α is a set of $(k+1)$-subsets of $\Omega\backslash\{\beta\}$ such that every $(t+1)$-subset of $\Omega\backslash\{\beta\}$ which is not contained in a block of S^*_β is in exactly one of the sets in X^ϕ_α. This means that X^ϕ_α is a set of blocks of S^*.

As $X^\psi_\alpha = X^\phi_\alpha$, we have now proved that ψ maps blocks of S^* to blocks of S^* and is therefore an automorphism of S^*. We also know that ψ maps α to β. This pair of elements of S^* were chosen arbitrarily, therefore, for each pair of elements in S^*, (α, β), there exists an automorphism which maps α to β. Therefore $\mathrm{Aut}(S^*)$ is transitive on Ω. □

3.3 Affine planes

In this section we introduce the idea of affine planes. This is crucial to our construction of M_{11} and M_{12} as the Steiner system we extend from in order to construct the Steiner systems which M_{11} and M_{12} act on is indeed an affine plane. The following theorems are exercises from [3].

This Lemma is is Exercise 6.2.3(ii) from [3].

Lemma 3.16. *Let $S = S(\Omega, \mathcal{B})$ be an $S(2, k, v)$ Steiner system. Then the following are equivalent:*

(i) $v = k^2$,

(ii) $r = k + 1$,

(iii) $b = k(k + 1)$,

(iv) *If α is a point in a block B, then there is a unique block which contains α and does not intersect B.*

Proof. We prove this by showing that they are all equivalent to (ii) and hence all equivalent.

We start with (ii) $\iff$ (i).

$$\begin{aligned} v = k^2 &\iff r = \frac{k^2-1}{k-1} = \frac{(k+1)(k-1)}{k-1} \\ &\iff r = k+1. \end{aligned}$$

Now we move on to (ii) $\implies$ (iii).

$$\begin{aligned} r = k+1 &\implies v = k^2 \ \text{ (from above)} \\ bk = vr &\implies bk = v(k+1) = k^2(k+1) \\ &\implies b = k(k+1) \ \text{ as } k \neq 0. \end{aligned}$$

Next we prove that (iii) $\implies$ (ii).
First note that

$$\begin{aligned} b = k(k+1) &\implies vr = k^2(k+1) \\ &\implies v = \frac{k^2(k+1)}{r}. \end{aligned}$$

Now notice

$$\begin{aligned} \frac{v-1}{k-1} = r &\implies v - 1 = rk - r, \\ v &= rk - r - 1, \\ k^2(k+1) &= r^2k - rk - r. \end{aligned}$$

We rearrange this into a quadratic equation.

$$(k-1)r^2 + r - k^2(k+1) = 0.$$

Now we substitute into the quadratic formula.

$$\begin{aligned} r &= \frac{-1 \pm \sqrt{1 + 4k^2(k-1)(k+1)}}{2(k-1)} \\ &= \frac{-1 \pm \sqrt{1 + 4k^2(k^-1)}}{2(k-1)} \\ &= \frac{-1 \pm \sqrt{1 + 4k^4 + 4k^2}}{2(k-1)} \\ &= \frac{-1 \pm \sqrt{(2k^2-1)^2}}{2(k-1)} \\ &= \frac{-1 \pm (2k^2-1)}{2(k-1)}. \end{aligned}$$

If we try the negative case we get

$$\begin{aligned} r &= \frac{-1-(2k^2-1)}{2(k-1)} \\ &= \frac{-k^2}{k-1} \leq 0. \end{aligned}$$

This is a contradiction as $r > 0$. If we now try the positive solution we get

$$\begin{aligned} r &= \frac{-1+(2k^2-1)}{2(k-1)} \\ &= \frac{k^2-1}{k-1} = k+1, \end{aligned}$$

which is the result we were looking for.

So we have proved (ii) $\iff$ (iii).

Moving on to (ii) $\implies$ (iv).
Let B be a block and $B = \{x_1, x_2, \ldots, x_k\}$. Then for each pair $\{\alpha, x_i\}$ with $1 \leq i \leq k$, there exists a distinct block which contains it. This is because otherwise there exists a block which is not B which contains both x_i and x_j where $i \neq j$. But this cannot be true as each 2-subset lies in only one block. Therefore α is in k distinct blocks which intersect B. We have assume though that $r = k+1$ therefore α lies in exactly one more block and this does not intersect B.

Finally we prove that (iv) $\implies$ (ii).
As above, there are k distinct blocks that contain α and intersect B. We have assumed that there is exactly one block containing α that does not intersect B, therefore α is contained in $k+1$ blocks. Our choice of α is arbitrary, hence each point in Ω lies in exactly $k+1$ blocks and so $r = k+1$. □

Definition 3.17. A Steiner system satisfying any of the properties in Lemma 3.16 is called an *affine plane*.

The following Theorem is Exercise 6.2.3(iii) from [3].

Theorem 3.18. *Let $S = S(\Omega, \mathcal{B})$ be an $S(2, k, v)$ Steiner system. If any of the properties in Lemma 3.16 are true, then the blocks of S can be partitioned into k+1 "parallel classes" each consisting of k blocks such that the blocks in a given parallel class are disjoint.*

Proof. The first thing we note is that if one of the properties in Lemma 3.16 is true then all of them are.

We prove the theorem by first building a parallel class $\mathcal{P}$ and then proving that it has size k. Then we prove that there are $k+1$ parallel classes.

To build $\mathcal{P}$ we use induction. The idea is that we have a set of pairwise disjoint blocks and we want to add another disjoint block.

To start we choose a block from $\mathcal{B}$ and call it B_0. Then we pick a point in $\Omega \backslash B_0$ and call it α_1. There are $k^2 - k$ choices for this point as $v = k^2$ and $|B_0| = k$. There exists a unique block which contains α_1 and does not intersect B_0 by Lemma 3.16. Call this block B_1. Therefore there exists a set of pairwise disjoint blocks $\bigcup_{i=0}^{1} B_i$.

For the inductive step we assume that there exists a set of pairwise disjoint blocks in S, $\bigcup_{i=0}^{l} B_i$ with $l \geq 2$.

While $\bigcup_{i=0}^{l} B_i \neq \Omega$, let α_{l+1} be any point in $\Omega \backslash \bigcup_{i=0}^{l} B_i$. There exists a unique block which contains α_{l+1} and does not intersect B_l by Lemma 3.16. Call this block B_{l+1}. The block B_{l+1} does not intersect any other block in $\bigcup_{i=0}^{l} B_i$. To prove this we assume that it does for contradiction. This would mean that there exists a $\gamma \in B_{l+1} \cap B_i$ for some $1 \leq i \leq l-1$. This implies that γ is in two distinct blocks, neither of which intersect B_l. This contradicts Lemma 3.16. Now we know that there exists a block B_{l+1} such that $B_{l+1} \cap B_i = \emptyset \ \ \forall\ 1 \leq i \leq l$ and therefore there exists a set of pairwise disjoint blocks in S, $\bigcup_{i=0}^{l+1} B_i$.

When $\bigcup_{i=0}^{n-1} B_i = \Omega$, we can see that $\Sigma_{i=0}^{n-1} |B_i| = |\Omega|$ since the B_i are pairwise disjoint. So we have n blocks, each of size k. This means that $nk = |\Omega|$ which implies that $n = k$. Therefore there are k disjoint blocks in $\mathcal{P}$. Our choice of B_0 was arbitrary so there are k disjoint blocks in each parallel class.

There cannot be any blocks which are disjoint with B_0 but not in $\mathcal{P}$. Assume for contradiction there is and call this block B_c. $\mathcal{P}$ has partitioned Ω and so every point in Ω lies in exactly one of the blocks $\mathcal{P}$. If we take any point x from B_c, then x lies in one of the blocks in $\mathcal{P}$, say B_x. This block is the unique block which contains x and does not intersect B_0. This means that $B_x = B_c$ and so B_c is in $\mathcal{P}$. So we get a contradiction.

Now we prove that no block lies in more than one parallel classes. This is equivalent to proving that if P_1 and P_2 are parallel classes, then $P_1 \cap P_2 = \emptyset$ or $P_1 = P_2$.

Let $B \in P_1$, $B \in P_2$ and $x \in \Omega \backslash B$. There exists a unique block B_x containing x such that $B_x \cap B = \emptyset$. This implies that $B_x \in P_1$ and $B_x \in P_2$. Our choice of x was arbitrary so $P_1 = P_2$.

The number of blocks b in Ω is k times the number of parallel classes. We know that $b = k(k+1)$ so the number of parallel classes is $k+1$.

□

Corollary 3.19. *Let $S = S(\Omega, \mathcal{B})$ be an $S(2, k, v)$ Steiner system. Each point in Ω lies in exactly one block from each parallel class.*

Proof. A parallel class of S partitions Ω.

□

4 Chapter 4

4.1 Affine groups

We now define certain groups along with some theorems about these groups without proof. These will help us with the construction of M_{11} and M_{12} and are taken from [3].

Definition 4.1. The affine geometry $AG_d(F)$ consists of points along with affine subspaces which are constructed from the vector space F^d of row vectors of dimension d over the field F.

- The points of the geometry are the vectors of F^d.
- The affine subspaces are the translates of the vector subspaces of F^d.

Definition 4.2. An *affine automorphism* is a permutation of the set of points of an affine geometry which maps each affine subspace to an affine subspace (of the same dimension).

Definition 4.3. An *affine transformation* is a simple form of an affine automorphism. For each linear transformation $a \in GL_d(F)$ and vector $v \in F^d$ we define the affine transformation $t_{a,v} : F^d \to F^d$ by

$$t_{a,v} : u \mapsto ua + v.$$

Each of these mappings is an automorphism of the affine geometry $AG_d(F)$.

Definition 4.4. The set of all $t_{a,v}$ $(a \in GL_d(F), v \in F^d)$ forms the *affine group* $AGL_d(F)$ of dimension $d \geq 1$ over F.

Theorem 4.5. *$AGL_d(F)$ is a 2-transitive subgroup of $Sym(F^d)$.*

For each field automorphism $\sigma \in Aut(F)$ there is a permutation of F^d defined by $t_\sigma : u \mapsto u^\sigma$ where σ acts component-wise on the vector u.

Lemma 4.6. *The mappings t_σ $(\sigma \in Aut(F))$ form a subgroup of $Sym(F^d)$ which we will call T.*

Definition 4.7. The *affine semi-linear transformations*, $A\Gamma L_d(F)$, is the group generated by T and $AGL_d(F)$. The elements of this group are the permutations of F^d of the form:

$$t_{a,v,\sigma} : u \mapsto u^\sigma a + v$$

where $a \in GL_d(F),\ v \in F^d$ and $\sigma \in Aut(F)$.

Theorem 4.8. *$A\Gamma L_d(F)$ is the full automorphism group of $AG_d(F)$ when $d \geq 2$.*

Corollary 4.9. *When $Aut(F) = 1$ (for example if $|F|$ is a prime or if $F = \mathbb{R}$ or $\mathbb{Q}$) then $A\Gamma L_d(F) = AGL_d(F)$.*

Definition 4.10. An *affine basis* for $AG_d(F)$ is a set $B = \{\alpha_0, \ldots, \alpha_d\}$ of $d+1$ points with the property that B is not contained in any $(d-1)$-dimensional affine subspace.

Theorem 4.11. *The affine group $AGL_d(F)$ acts regularly on the set of affine bases of $AG_d(F)$.*

Corollary 4.12. *The affine group $AGL_d(F)$ is transitive on the set of affine bases of $AG_d(F)$.*

4.2 The Affine Plane $AG_2(3)$

We now do a detailed study of the affine plane $AG_2(3)$. We do this because we will later build the Steiner systems M_{11} and M_{12} from $AG_2(3)$. We prove several geometric properties of $AG_2(3)$ along with theorems about $\mathrm{Aut}(AG_2(3))$. This leads us to proving that there is a unique $S(2, 3, 9)$ Steiner system up to isomorphism and that this Steiner system is indeed $AG_2(3)$. We follow the exercises and theorem of [3] in this subsection.

The affine plane $AG_2(3)$ is the set of 9 points in the 2-dimensional vector space over the field $\mathbb{F}_3 = \{0, 1, 2\}$. To simplify, we write ij to represent (i, j), where $i, j \in \{0, 1, 2\}$, for the elements of $AG_2(3)$.

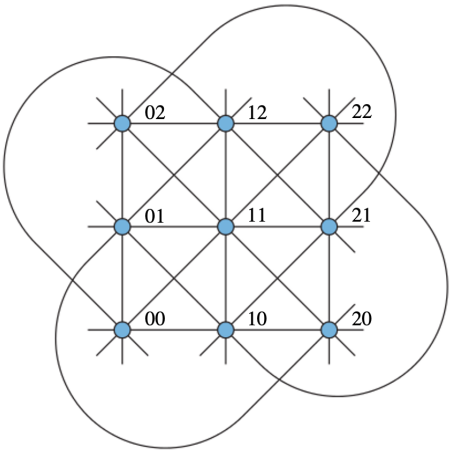

Figure 2: $AG_2(3)$

$AG_2(3)$ is an affine plane with $9 = 3^2$ points so is an $S(2, 3, 9)$ Steiner system. This means it has $3(3+1) = 12$ lines, each of these lines contains exactly 3 points and every pair of points lies on a unique line. By Theorem 3.18 we can partition these 12 lines into $3 + 1 = 4$ parallel classes, each consisting of 3 lines, namely:

00 10 20	00 01 02	00 11 22	00 12 21
01 11 12	10 11 12	01 12 20	01 10 22
02 12 22	20 21 22	02 10 21	02 11 20

The following Theorem is Exercise 6.3.1 of [3].

Theorem 4.13. *In $AG_2(3)$ there are:*

(i) 72 *triangles;*

(ii) 54 *quadrangles (sets of* 4 *points with no* 3 *collinear);*

(iii) 4 *triangles in each quadrangle;*

(iv) 3 *quadrangles containing a given triangle.*

Proof. (i) There are 12 lines we want to avoid, so we do $\binom{9}{3} - 12 = 84 - 12 = 72$.

(ii) The number of 4-subsets of the points of $AG_2(3)$ is $\binom{9}{4} = 126$. We want to find sets of 4 which contain 3 linear points and then exclude these. To do this we pick a line and a point which is not on this line. There are $12 \times (9 - 3) = 72$ ways to do this. $126 - 72 = 54$.

(iii) No 3 points in a quadrangle are collinear therefore any 3 points in a quadrangle form a triangle. $\binom{4}{3} = 4$.

(iv) Take a triangle. There are $9-3 = 6$ choices of points left to make a quadrangle. Each pair of points in the triangle is on a unique line each with a third point on it we do not want in the quadrangle (otherwise we have at three collinear points). There are $\binom{3}{2} = 3$ pairs in a triangle and therefore 3 points to avoid. $6 - 3 = 3$ so there are 3 choices of how to extend a triangle into a quadrangle and therefore 3 quadrangles containing a given triangle.

□

Lemma 4.14. *Every set of 5 points in $AG_2(3)$ contains at least one line.*

Proof. Call a set of 5 points F. We first assume that F does not contain full a line by way of contradiction. There are $\binom{5}{2}$ pairs of points in any set of size 5 and therefore 10 different lines incident with any 2 points of F. None of the third points of any of

these lines can lie in F otherwise we have a full line in F. This means that all the third points are outside of F. A maximum of 2 lines in F can share a third point and the pairs of points that are incident to these lines must be disjoint. Otherwise these lines share 2 points and are therefore the same line. This means that there are a minimum of $10/2 = 5$ points outside of F. But there are only $9 - 5 = 4$ points left in Ω. Therefore we get a contradiction. □

The following Theorem is Exercise 6.3.3 of [3].

Theorem 4.15. *Every set of five points in $AG_2(3)$ contains at least one quadrangle.*

Proof. By Lemma 4.14, this set of 5 points $F := \{x_1, \ldots, x_5\}$ contains at least one line. Call this line l and without loss of generality, let $l = \{x_3, x_4, x_5\}$. To make our quadrangle we can only choose a maximum of 2 of the elements on this line, otherwise we have 3 collinear points in F. By leaving out one of the elements on l this forces to use all the other 4 elements of F and specifically the 2 elements of $F\backslash l$, x_1 and x_2. Neither x_1 nor x_2 can make a full line with just itself and any 2 elements of l as any 2 elements we choose from l are already on a line together and this line is unique by the definition of an affine plane. This means that the only lines we need to avoid are ones that have both x_1 and x_2. This pair is on a unique line and therefore there is only one point to avoid. If this point is in l then we simply pick the other 2 points of l to complete our quadrangle as shown in Figure 3. Otherwise we can pick any 2 elements of l as shown in Figure 4. □

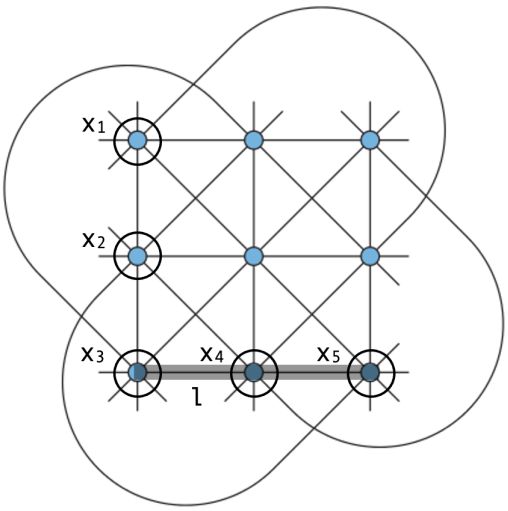

Figure 3

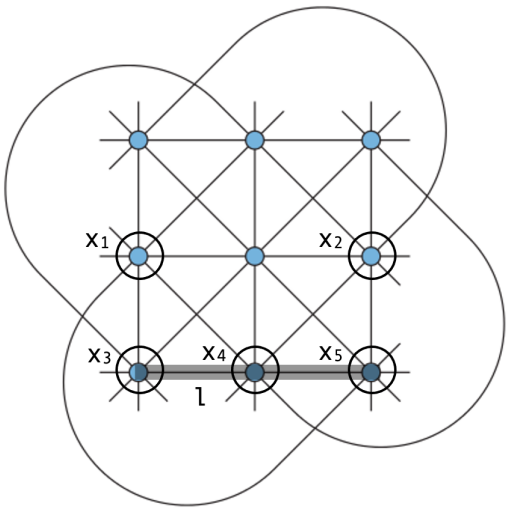

Figure 4

Lemma 4.16. *The automorphism group of $AG_2(3)$ is $AGL_2(3)$.*

Proof. This follows directly from Theorem 4.8 and Corollary 4.9. □

Lemma 4.17. *$AGL_2(3)$ induces an action on the set of 4 parallel classes.*

Proof. Let l_1 and l_2 be lines in $AG_2(3)$ and let $g \in AGL_2(3)$. From this we know that l_1^g and l_2^g are both lines in $AG_2(3)$ (blocks are mapped to blocks). We also know that $(l_1 \cap l_2)^g = (l_1^g \cap l_2^g)$ as g is an automorphism of $AG_2(3)$. This means that l_1 and l_2 are parallel if and only if l_1^g and l_2^g are parallel. □

The following Theorem is Exercise 6.3.2 of [3].

Theorem 4.18. *$AGL_2(3)$ induces S_4 on the set of 4 parallel classes.*

Proof. First we label the parallel classes as follows:

a	b	c	d
00 10 20	00 01 02	00 11 22	00 12 21
01 11 12	10 11 12	01 12 20	01 10 22
02 12 22	20 21 22	02 10 21	02 11 20

Let $\mathcal{P} = \{a, b, c, d\}$. $\mathrm{Sym}(\mathcal{P}) = \langle (a\ b), (a\ b), (a\ c) \rangle$ as the set of all transpositions in S_4 is enough to generate the whole of S_4 and one can generate this set using the three transpositions $\{(a\ b), (a\ c), (a\ d)\}$ using conjugation as shown in [2]. This means that it suffices to show that there exists elements of $AGL_2(3)$ that induce $(a\ b)$, $(a\ c)$ and $(a\ d)$ on $\mathcal{P}$.

We first try to find an element G_1 of $AGL_2(3)$ which induces $(a\ b)$ on $\mathcal{P}$.

We state that a possibility of G_1 is

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

G_1 is clearly in $AGL_2(3)$ as it is in $GL_2(3)$.

By Lemma 4.17 it is enough to show that G_1 maps an element a to an element b, vice versa and G_1 maps an element c to an element c (this forces d to be mapped to d.

$$\begin{bmatrix} 0 & 0 \end{bmatrix} G_1 = \begin{bmatrix} 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \end{bmatrix} G_1 = \begin{bmatrix} 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 \end{bmatrix} G_1 = \begin{bmatrix} 0 & 2 \end{bmatrix};$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} G_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 \end{bmatrix} G_1 = \begin{bmatrix} 2 & 0 \end{bmatrix};$$

$$\begin{bmatrix} 1 & 1 \end{bmatrix} G_1 = \begin{bmatrix} 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 2 \end{bmatrix} G_1 = \begin{bmatrix} 2 & 2 \end{bmatrix}.$$

This shows that G_1 maps 00 10 20 to 00 01 02 and vice versa. It also shows that 00 11 22 is mapped to itself. This proves that G_1 induces $(a\ b)$ on $\mathcal{P}$.

There also exists elements $G_2, G_3 \in AGL_2(3)$ such that they induce $(a\ c)$ and $(a\ d)$ on $\mathcal{P}$ respectively.

$$G_2 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix},\ G_3 = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}.$$

We can prove that these do indeed work by following the same logic as above.

□

Theorem 4.19. *There is a unique $S(2,3,9)$ Steiner system up to isomorphism. This is $AG_2(3)$.*

Proof. This proof follows that of [3].

Let $S = (\Omega, \mathcal{B})$ be an $S(2,3,9)$ Steiner system. In anticipation of the result, we will refer to its blocks as "lines". By Theorem 3.18 we know that the lines of S can be partitioned into 4 parallel classes, each containing 3 points. Pick one of these, call it R and write down its lines as 3 rows, then pick another of the parallel classes and call it C.

Take a line B_C in C and a line B_R in R. We claim that these lines intersect in exactly one point. To see this, notice that $|B_C \cap B_R| \geq 1$, otherwise these lines would be parallel and therefore the line in C would also be in R. However, we know that parallel classes are disjoint. If $|B_C \cap B_R| \geq 2$, then this would imply that $B_C = B_R$ as any pair of points lie in exactly one line. Therefore each line in C intersects each line in R exactly once.

No two pair of lines (B_C, B_R) intersect at the same place. This is because otherwise two lines from C (and two lines R) would intersect. This is impossible as C is a parallel classes and it's lines cannot intersect one another.

Each point in the Steiner system is at exactly one of these intersections. This is because there are 3 rows and 3 columns which each intersect with each other once each and $3 \times 3 = 9$. Plus we have shown that the intersections are distinct.

This means that we can rearrange the points in the rows so that the columns form the lines of a second parallel class, C.

Call the rows B_{R1}, B_{R2}, B_{R3} from top to bottom and the columns B_{C1}, B_{C2}, B_{C3} from left to right. We pick the point x_1 from the intersection of B_{R1} and B_{C1} and the point x_2 from the intersection of B_{R2} and B_{C2} (different rows and columns for both of these points). These two points lie in exactly one line B. To find this line we must find the third point x_3. The point x_3 cannot be in any of $B_{R1}, B_{R2}, B_{C1}, B_{C2}$, i.e. it cannot lie in the same row or column as either given point. To prove this we assume for contradiction that x_3 is in B_{R1} for example. The point x_1 is also in B_{R1} so our new line $B = B_{R1}$ as any pair of points lie in a unique line. This cannot be

true as $x_2 \notin B_{R1}$. Similar proofs follow for B_{R2}, B_{C1}, B_{C2} as they either contain x_1 or x_2. The point x_3 must be at the intersection of one row line and one column line so it must be at the intersection of B_{R_3} and B_{C_3}. This makes a diagonal line.

We can now assume that 7 of the lines of S can be displayed as in Figure 5. There are $12 - 7 = 5$ more lines needed to complete the Steiner system.

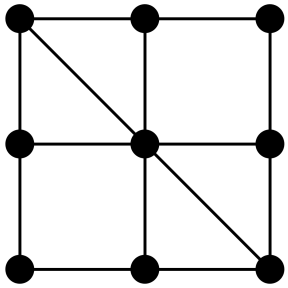

Figure 5

For the final lines we follow this set of steps 5 times.
Take 2 points not already joined by a line. This means that they are on different rows and columns as discussed above. The third point needed to make a line must be on a different row and column to the other two, therefore there is only one choice on how to make the line with two given points.

We do this 5 times as we have 6 points left. $\binom{6}{2} = 15$ and there are 3 points on every line so we must divide 15 by 3, which gives us 5. We know we don't get stuck as we know that $AG_2(3)$ exists.

□

4.3 The Extension of $AG_2(3)$

In this subsection we extend the $S(2, 3, 19)$ Steiner system to an $S(3, 4, 10)$. This is because the way we construct the Steiner system on which M_{11} acts, namely $S(4, 5, 11)$, is by constructing a one-point extension of $S(3, 4, 10)$. Therefore we need to construct an $S(3, 4, 10)$ Steiner system first. We discuss the quadrangles of $AG_2(3)$ as these are needed when constructing the blocks of $S(3, 4, 10)$. Once we have constructed an $S(3, 4, 10)$ Steiner system, we then prove that it is unique up to isomorphism and discuss properties of its automorphism group. This subsection follows [3].

We want to extend $AG_2(3)$ to an $S(3, 4, 10)$ Steiner system (called W_{10}) by adding a new point α and defining appropriate new blocks. There is no reason this should

work so we must construct it. The Steiner system W_{10} will have $r = (9 \cdot 8)/(3 \cdot 2) = 12$ blocks containing each point, $b = (10 \cdot 12)/4 = 30$ blocks and each triple will be contained in a unique block. The blocks of W_{10} which contain α will be of the form $L \cup \{\alpha\}$ where L is a line of $AG_2(3)$. These 12 blocks $L \cup \{\alpha\}$ cover all triples which include α as well as all collinear triples of points of $AG_2(3)$. This means that the remaining blocks of W_{10} must cover all the triangles of $AG_2(3)$ once each. These blocks consist of all sets of 4 points from $AG_2(3)$ (as all the blocks containing α have already been defined) of which no 3 are collinear (the collinear triples are already in the blocks $L \cup \{\alpha\}$ and any three points are in a unique block). This means we are looking for a set of $30 - 12 = 18$ (b - number of blocks of the form $L \cup \{\alpha\}$) quadrangles to cover the 72 triangles of $AG_2(3)$ once each. We shall show that there are exactly 3 such sets of 18 quadrangles and these 3 sets partition the set of all 54 quadrangles of $AG_2(3)$.

Lemma 4.20. *$AGL_2(3)$ is transitive on quadrangles in $AG_2(3)$.*

Proof. A quadrangle of $AG_2(3)$ satisfies the conditions to be an affine basis for $AG_2(3)$. By Corollary 4.12, $AGL_2(3)$ acts transitively on the set of affine bases of $AG_2(3)$ and therefore does so on the set of quadrangles of $AG_2(3)$. □

Theorem 4.21. *For each quadrangle in $AG_2(3)$, there are 6 lines joining its 4 point in pairs. The lines of a quadrangle can be separated into 4 sets; 2 of size one and 2 of size 2, such that each set is in a different parallel class.*

Proof. We only have to look at one quadrangle as the $AGL_2(3)$ is transitive on quadrangles by Lemma 4.20. So we look at the quadrangle 00 01 10 11 as shown in Figure 6.

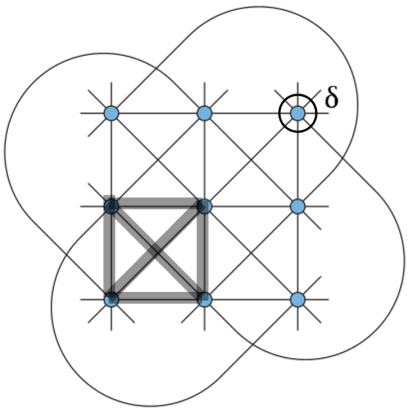

Figure 6

It is clear to see from this that the quadrangle has 2 lines in parallel class a, 2 in b, one in c and one in d. □

Definition 4.22. A quadrangle Ξ has *type* $\{x, y\}$ if x and y are the 2 parallel classes that each contain 2 of the 6 lines of Ξ.

Corollary 4.23. *The vertices of a quadrangle of type* $\{x, y\}$ *lie in 3 lines of the quadrangle each, with* 2 *of them being in* x *and* y*.*

Proof. We only have to look at one quadrangle as the automorphism group of $AG_2(3)$ is transitive on quadrangles. Then we simply look at Figure 6 to see this is true. □

The following Theorem is Exercise 6.3.4 in [3].

Theorem 4.24. *For any quadrangle* Ξ *of* $AG_2(3)$*:*

(i) *There is a unique point* δ *outside of* Ξ *which lies on two distinct lines of* Ξ*. This point is called the diagonal point of the quadrangle.*

(ii) *There is a unique quadrangle* Ξ^* *disjoint from* Ξ*. Furthermore,* Ξ *and* Ξ^* *have the same diagonal point.*

(iii) *If* Ξ *is a quadrangle of type* $\{a, b\}$*, and* γ *is a point outside* Ξ *such that the only quadrangles contained in* $\Xi \cup \{\gamma\}$ *are of type* $\{a, b\}$ *or* $\{c, d\}$*, then* γ *is the diagonal point of* Ξ*.*

Proof. (i) Assume Ξ has type $\{a, b\}$. This means that Ξ has exactly one line in parallel c and one in d. Call them l_1 and l_2 respectively. The lines l_1 and l_2 have exactly one point in common as if they had none, they'd be in the same parallel class and if they had 2 or 3 then they would be the same line. Call this point of intersection δ. This point δ is not a vertex of Ξ by Corollary 4.23 and the fact δ lies in both lines from c and d . The 4 other lines of Ξ meet in pairs at the vertices of Ξ and once again cannot meet in pairs at any other points (as either they have already met once at a vertex or are parallel and therefore never meet). This shows that δ is unique. This is shown in Figure 6.

(ii) Assume Ξ has type $\{a, b\}$. There are 12 lines in $AG_2(3)$ and 6 of these are in Ξ. This leaves 6 lines not in Ξ. Similarly, there are 9 points in $AG_2(3)$ and 4 of these are in Ξ, so there are 5 points not in Ξ. By Theorem 4.15 these five points in $AG_2(3)\backslash\Xi$ contain a quadrangle. Call this Ξ^*. As Ξ^* is quadrangle, it also contains 6 lines. These are the lines in $AG_2(3)\backslash\Xi$ as Ξ^* is disjoint from Ξ. Let δ be the diagonal point of Ξ. The point δ lies in one of the five points of $AG_2(3)\backslash\Xi$ and δ lies in 4 lines as $r = 4$. Two of these are in Ξ by the definition

of δ which means that the other 2 are in Ξ^*. One of the lines in Ξ that passes through δ is from parallel class c, and the other in d by part (i). This means, by Corollary 3.19, that one of the lines of Ξ^* that passes through δ is from parallel class a and the other in b. Each vertex in a quadrangle lies in 3 lines of the quadrangle by Corollary 4.23. The point δ is only in 2 lines of Ξ^*, so cannot be a vertex of this quadrangle. Since δ lies outside of Ξ^* as well as in 2 distinct lines of Ξ^*, δ is the diagonal point of Ξ^*.

(iii) We know that $AGL_2(3)$ acts transitively on quadrangles and so we only need to prove this for one quadrangle. Consider the quadrangle 00 01 10 11 as shown in Figure 6. First we consider the point 20 as a possibility for γ. The quadrangle 01 11 10 20 is in $\Xi \cup \{\gamma\}$ and is of type $\{a, d\}$. Therefore $\gamma \neq 20$ and by symmetry, $\gamma \neq 02$. Now we consider the point 21 as a possibility for γ. The quadrangle 00 01 11 21 is in $\Xi \cup \{\gamma\}$ and is of type $\{a, c\}$. Therefore $\gamma \neq 21$ and by symmetry, $\gamma \neq 12$. Finally we consider the point 22 as a possibility for γ. The only quadrangle we can form in $\Xi \cup \{\gamma\}$ is Ξ as once we include 22 then any choice of point x_1 from Ξ forces us to leave out the other point on the line of γ and x_i. This means we must choose the remaining 2 points of Ξ, but these are on a line together with γ. The quadrangle Ξ is of type $\{a, b\}$ and so $\gamma = 22$. It is easy to see that γ is the diagonal point of Ξ.

□

Corollary 4.25. *If the parallel classes of $AG_2(3)$ are $\{a, b, c, d\}$ and a quadrangle Ξ has type $\{a, b\}$, then the unique quadrangle Ξ^* disjoint from Ξ has type $\{c, d\}$.*

Proof. By Theorem 4.24(ii) the diagonal point δ of Ξ^* lies in two lines of Ξ^* and these are in parallel classes a and b (one in each). We proved in Theorem 4.24(i) that the 2 lines of a quadrangle of type $\{x, y\}$ that intersect its diagonal point cannot be in the parallel classes x or y. This means that Ξ^* must be of type $\{c, d\}$. □

The set $\{a, b, c, d\}$ of 4 parallel classes of $AG_2(3)$ can be partitioned in 3 different ways into pairs of 2-subsets: $ab|cd$, $ac|bd$ and $ad|bc$.

Definition 4.26.
- Z_1 = the set of all quadrangles of $AG_2(3)$ which either have type $\{a, b\}$ or $\{c, d\}$;
- Z_2 = the set of all quadrangles of $AG_2(3)$ which either have type $\{a, c\}$ or $\{b, d\}$;
- Z_3 = the set of all quadrangles of $AG_2(3)$ which either have type $\{a, d\}$ or $\{b, c\}$.

Lemma 4.27. *Each quadrangle of $AG_2(3)$ belongs to exactly one of these parallel classes.*

Proof. Quadrangles can only be of one type and all the types belong to exactly one of the sets Z_i for $i \in \{1, 2, 3\}$. □

Lemma 4.28. *Each of the sets Z_i for $i \in \{1, 2, 3\}$ contains 18 of the 54 quadrangles of $AG_2(3)$.*

Proof. $AGL_2(3)$ maps quadrangles to quadrangles and also maps parallel classes to parallel classes. In fact we know now that $AGL_2(3)$ induces S_4 on the parallel classes of $AG_2(3)$ by Theorem 4.18. This means that there are the same number of quadrangles of each type. There are 6 types of quadrangles and therefore $54/6 = 9$ of each. Each set Z_i ($i \in \{1, 2, 3\}$) contains quadrangles of 2 different types and therefore there are 18 quadrangles in each Z_i ($i \in \{1, 2, 3\}$). □

Lemma 4.29. *Each pair of distinct points $\{\sigma, \rho\}$ in $AG_2(3)$ lies in exactly:*

(i) 6 *triangles;*

(ii) 9 *quadrangles.*

Proof. (i) We must avoid any point that would form a full line with $\{\sigma, \rho\}$. There is only one of these, which leaves 6 points left in $AG_2(3)$ and hence 6 triangles containing our pair.

(ii) We start with our original pair again and try to find pairs of points that when included with $\{\sigma, \rho\}$ in a set, does not contain any 3 collinear points. As above we must avoid any point that would form a full line with $\{\sigma, \rho\}$. There is only one of these, which leaves 6 points left in $AG_2(3)$. This means are $\binom{6}{2} = 15$ choices for distinct pairs to add to our original pair in order to make a set of 4. However we want to not add any pairs that will form a line with either σ or ρ. The point σ lies on 3 lines that do not contain ρ and ρ lies on 3 lines that do not contain σ as both of these points lie on 4 lines each and one of these lines contains $\{\sigma, \rho\}$. Obviously these 2 sets of 3 lines do not intersect. Therefore we want to avoid the pairs that make up these 6 lines. There are no more pairs of points to avoid so we have $15 - 6 = 9$ quadrangles containing $\{\sigma, \rho\}$.

□

Theorem 4.30. *Each set $S = Z_i$ with $i \in \{1, 2, 3\}$ has the property:*

($*$) *Each triangle of $AG_2(3)$ is in a unique quadrangle from S.*

Conversely, these are the only sets of 18 quadrangles with this property.

Proof. This proof follows that of [3].

First we show that Z_i with $i \in \{1, 2, 3\}$ has property $(*)$. By symmetry we only need to consider the case Z_1 with quadrangles of type $\{a, b\}$ or $\{c, d\}$. Consider any triangle T. The 3 lines of the triangle must all be in different parallel classes as each line intersects the other 2 and no 2 lines in the same parallel class intersect. This means that 3 of the 4 parallel classes are represented by this triangle and one is not. Assume this class is d. We now extend T to a quadrangle by adding a point π and 3 new lines from π to each of the vertices of T. The 3 lines through π that are part of this quadrangle all lie in different classes. This means that d can be at most one of these new lines and therefore we can have a maximum of one line in the quadrangle which lies in d. This means that the quadrangle we have made cannot be of type $\{a, d\}, \{b, d\}$ or $\{c, d\}$. We only care that our quadrangle is not of type $\{c, d\}$ as this means that T is not contained in any quadrangle of type $\{c, d\}$.

Now we prove that there does exist a unique quadrangle of type $\{a, b\}$ in which T lies. Call the vertices of T t_1, t_2, t_3 where the line l_1 through t_1 and t_2 is in class a, and the line l_2 through t_1 and t_3 is in class b. We are trying to construct a quadrangle of type $\{a, b\}$ and so we need one more line of class a and one of b to connect to the final vertex. The point t_1 is already on a line of class a, l_1, and b, l_2 so we will be adding the new lines to t_2 and t_3. The point t_2 is already in a line of class a, l_1, with t_1 so we cannot have another connecting it to a new vertex. Similarly t_3 cannot be in another line of class b due to $t_3 \in l_2$. There is a unique line l_3 of class a through t_3 and a unique line l_4 of class b through t_2. These 2 lines are distinct and not in the same class so intersect at exactly one point ρ. This is displayed in Figure 7. The 4-set $\Xi := \{t_1, t_2, t_3, \rho\}$ is therefore the unique quadrangle of type $\{a, b\}$ containing T. As noted above, T is not contained in any quadrangles of type $\{c, d\}$ so we have proved that Z_1 satisfies property $(*)$.

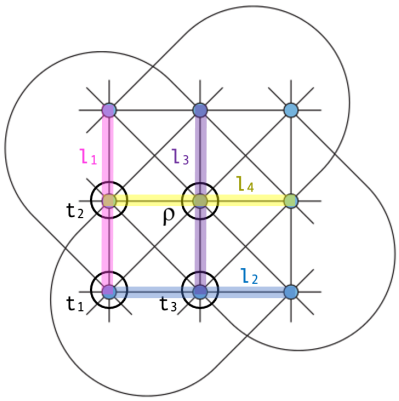

Figure 7

To prove the converse, let S be a set of 18 quadrangles which satisfies property $(*)$. For each pair of distinct points $\{\sigma, \rho\}$ we define $Q(\sigma, \rho)$ to be the set of all quadrangles in $AG_2(3)$ which contain these points. There are 9 of these by Lemma 4.29. Let us pick a specific pair of points and consider their quadrangles. The 9 quadrangles of $Q(00, 01)$ can be constructed as in the proof of Lemma 4.29 by simply avoiding adding pairs to $(00, 01)$ that would not make a quadrangle. The pairs added to $(00, 01)$ to make the quadrangles of $Q(00, 01)$ are:

$$\Xi_1 : 10, 11; \quad \Xi_2 : 10, 12; \quad \Xi_3 : 10, 21; \quad \Xi_4 : 11, 12; \quad \Xi_5 : 11, 20;$$

$$\Xi_6 : 12, 22; \quad \Xi_7 : 20, 21; \quad \Xi_8 : 20, 22; \quad \Xi_9 : 21, 22.$$

We know that there are 6 triangles which contain the points 00 and 01 by Lemma 4.29. Each quadrangle which contains 00 and 01 contains 2 triangles which contain 00 and 01 as we can choose any of the 2 other points of the quadrangle to make the triangle. The triangles cannot be in more than one quadrangle which contains 00 and 01 by property $(*)$ and so S contains exactly 3 of the 9 quadrangles $\{\ \Xi_i \mid 1 \leq i \leq 9\ \}$ above and these 3 quadrangles only intersect at 00 and 01. From this we can easily see that the only possibilities for $S \cap Q(00, 01)$ are: $\{\Xi_1, \Xi_6, \Xi_7\}$, $\{\Xi_2, \Xi_5, \Xi_9\}$, $\{\Xi_3, \Xi_4, \Xi_8\}$ or $\{\Xi_3, \Xi_5, \Xi_6\}$. The first 3 of these sets, lie in Z_i for some $i \in \{1, 2, 3\}$. One can see this from drawing out the quadrangles and looking at their respective types.

For the last of the triples there is no i such that it lies in Z_i. We can write this triple as $N :=$ 00 01 : 10 21; 11 20; 12 22. We shall show that N cannot be extended to a set S satisfying property $(*)$ and so we can remove N as a possibility for $S \cap Q(00, 01)$.

We calculate the possibilities for $S \cap Q(00, 10)$. To do this we consider the list of triples of quadrangles which give a covering of the 6 triangles which contain {00 10} using the same method as above.

1. 00 10 : 01 11; 21 22; 02 12

2. 00 10 : 01 21; 11 02; 12 22

3. 00 10 : 01 12; 21 11; 02 22

4. 00 10 : 01 12; 11 02; 21 22

Each of the triples $1 - 4$ contains a quadrangle which intersects one of the quadrangles of N in a triangle. For example, for the triples 1, 3 and 4 take the triangle 00 01 10 which is already in quadrangle 00 01 10 21. For the triple 2 we

take the triangle 00 12 22. This triangle is in both the quadrangle 00 10 12 22 (from triple 2) and the quadrangle 00 01 12 22 (from N). This would mean that S does not have property $(*)$ and so none of these possibilities for $S \cap Q(00, 10)$ is consistent with $S \cap Q(00, 01) = N$.

This mean that we only need to consider $\{\Xi_1, \Xi_6, \Xi_7\}$, $\{\Xi_2, \Xi_5, \Xi_9\}$ and $\{\Xi_3, \Xi_4, \Xi_8\}$ for $S \cap Q(00, 01)$. So we now know that $S \cap Q(00, 01) \subseteq Z_i$ for some $i \in \{1, 2, 3\}$.

$AGL_2(3)$ acts 2-transitively on $AG_2(3)$ by Theorem 4.5. Plus $AGL_2(3)$ leaves the property $(*)$ invariant as any elements of $AGL_2(3)$ will map quadrangles to quadrangles and triangle to triangles (cannot map non-collinear points to collinear points). This implies the following more general fact: For each set $\{\sigma, \rho\}$ of distinct points, there exists an i such that $S \cap Q(\sigma, \rho) \subseteq Z_i$. So, it remains to show that i is independent of our choices of $\{\sigma, \rho\}$.

Now we suppose that $\{\sigma, \rho\}$ and $\{\sigma, \rho'\}$ are pairs such that $\rho \neq \sigma \neq \rho'$, and also that $S \cap Q(\sigma, \rho) \subseteq Z_i$ and $S \cap Q(\sigma, \rho') \subseteq Z_j$. We claim that $i = j$.

We can choose triangles T and T' such that $\{\sigma, \rho\} \subseteq T$, $\{\sigma, \rho'\} \subseteq T'$ and $|T \cap T'| = 2$ (i.e. $T \cap T' = \{\sigma, \tau\}$ where τ is the third point in both T and T'). Let Ξ and Ξ' be the quadrangles in S containing T and T' respectively. Then $\Xi \in Z_i$ as $\Xi \in \{S \cap Q(\sigma, \rho)\} \subseteq Z_i$. We also know that $\Xi' \in Z_j$. Plus both of these quadrangles are in $S \cap Q(T \cap T') \subseteq Z_x$ by the construction of T and T'. We know that any quadrangle can only be in one Z_i, so from this we know that $i = x = j$ as required.

As the argument works for $\{\sigma, \rho\}$ and $\{\sigma, \rho'\}$, then it works for any choice of ρ' in $\{\sigma, \rho'\}$. But then one can change σ, whilst keeping ρ fixed in $\{\sigma, \rho\}$, to see that it works for all pairs. □

Corollary 4.31. *All Steiner systems which are one-point extensions of $AG_2(3)$ are isomorphic.*

Proof. This proof follows that of [3].

It follows from Theorem 4.30 that when we extend $AG_2(3)$ by adding a point α, the 18 blocks which do not contain α can only be chosen in 3 ways: Z_1, Z_2 or Z_3. We know from Theorem 4.18 that $AGL_2(3)$ induces S_4 on the set of 4 parallel classes of $AG_2(3)$. This means that $AGL_2(3)$ induces S_3 on the set of 3 partitions $\{ab \mid cd,\ ac \mid bd,\ ad \mid bc\}$. Thus $AGL_2(3)$ acts transitively on $\{Z_1, Z_2, Z_3\}$, which means that all the one-point extensions of $AG_2(3)$ are isomorphic. □

Lemma 4.32. *The order of $GL_2(3)$ is 48.*

Proof. Let $M \in GL_2(3)$ and

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We have 8 choices for $(a\ b)$ as we can choose any element of $(\mathbb{F}_3)^2\backslash\{(0\ 0)\}$. For $(c\ d)$ we can choose any element of $(\mathbb{F}_3)^2\backslash\{(0\ 0)\}$ which is not a scalar multiple of $(a\ b)$. Our only scalars are 1 and 2, therefore we have $8-2=6$ choices for $(c\ d)$. Therefore $|GL_2(3)| = 8 \cdot 6 = 48$.

Another similar explanation is found in [7]. □

Lemma 4.33. *The order of $AGL_2(3)$ is $9 \cdot 8 \cdot 6$.*

Proof. We know that

$$AGL_2(3) = \{\ t_{a,v} \mid t_{a,v}(u) = ua + v,\ u \in GL_2(3),\ v \in (\mathbb{F}_3)^2\}.$$

Let T be the group of translations in $AGL_2(3)$, i.e. $(\mathbb{F}_3)^2$.
By Lemma 4.32 we know that $|GL_2(3)| = 48$ and we also know $|T| = 3^2 = 9$.
Therefore $|AGL_2(3)| = 9 \cdot 48 = 9 \cdot 8 \cdot 6$.

□

Theorem 4.34. *Up to isomorphism, there is a unique $S(3,4,10)$ Steiner system which we shall denote by W_{10}.*

Proof. This proof follows that of [3].

Let $S = (\Omega, \mathcal{B})$ be an $S(3,4,10)$ Steiner system W and choose an element $\alpha \in W$. By Theorem 3.12 there exists a contraction of W by α which is an $S(2,3,9)$ Steiner system. By Theorem 4.19 there is only one such geometry, namely Corollary 4.31 is therefore determined up to isomorphism. We shall now denote W by W_{10}. □

Theorem 4.35. *Aut(W_{10}) is transitive and has order $10 \cdot 9 \cdot 8 \cdot 2$.*

Proof. This proof follows that of [3].

The group W_{10} is a one-point extension of $AG_2(3)$. The group $AG_2(3)$ is determined uniquely up to isomorphism by Theorem 4.19 and there is a unique way of choosing the blocks of $AG_2(3)$ up to the action of $AGL_2(3)$ as proved in the previous section. Therefore by Theorem 3.15, $\mathrm{Aut}(W_{10})$ is transitive on the points of (W_{10}).

The stabiliser of a point α in $\mathrm{Aut}(W_{10})$ is an automorphism group of W_α by Theorem 3.13 and therefore by Theorem 3.14, $(\mathrm{Aut}(W_{10}))_\alpha$ leaves one of the Z_i invariant. Thus $(\mathrm{Aut}(W_{10}))_\alpha$ is isomorphic to the subgroup of $AGL_2(3)$ which fixes one of the Z_i, say Z_1. This subgroup is simply the stabiliser of the partition $P = \{ab \mid cd\}$ of the 4 parallel classes and so it is a subgroup of index 3 in $AGL_2(3)$ as $AGL_2(3)$ induces S_3 on the set of 3 partitions of parallel classes. By Lemma 4.33, the order of $AGL_2(3)$ is $9 \cdot 8 \cdot 6$. By the orbit-stabiliser property we know that

$$|(\mathrm{Aut}(W_{10}))_\alpha| = |(AGL_2(3))_P| = |(AGL_2(3))|/|P^{AGL_2(3)}| = (9 \cdot 8 \cdot 6)/3 = 9 \cdot 8 \cdot 2.$$

As $\mathrm{Aut}(W_{10})$ is transitive $|\alpha^{\mathrm{Aut}(W_{10})}| = 10$, and so

$$|\mathrm{Aut}(W_{10})| = |\alpha^{\mathrm{Aut}(W_{10})}| \cdot |(\mathrm{Aut}(W_{10}))_\alpha| = 10 \cdot 9 \cdot 8 \cdot 2.$$

□

The following Lemma is Exercise 6.3.5 in [3].

Lemma 4.36. *Let H be the stabiliser in $AGL_2(3)$ of the partition $ab \mid cd$. Then H has an index 2 subgroup which is sharply 2-transitive on the points of $AG_2(3)$.*

Proof. The group H acts as S_2 on the partitions $ac|bd$ and $ad|bc$ as H stabilises $ab|cd$ and $AGL_2(3)$ acts as S_3 on the set of all 2-set partitions as discussed in the proof of Corollary 4.31.

We consider the stabiliser of all three partitions $ab|cd,\ ac|bd$ and $ad|bc$ and call this group S. By the orbit-stabiliser property

$$|H : S| = |\{ac|bd\}^H| = 2.$$

We now show how to construct S.
First we define a group $H^* = H_{00}$. From this we know that, $H^* < H$ and that H^* is the stabiliser of the partition $ab|cd$ in $GL_2(3)$.

$$|H^*| = |GL_2(3)|/|\{ab|cd\}^{H^*}| = 48/3 = 16.$$

Consider the point stabiliser of 00 in S, i.e. S_{00}. This group is the stabiliser in $GL_2(3)$ of all 3 partitions $ab|cd, ac|bd$ and $ad|bc$. Let $S^* = S_{00}$. Then

$$|S^*| = |H^*|/|H^* : S^*| = 16/2 = 8.$$

We now find these 8 matrices. In order for S^* to stabilise all 2-set partitions, the only permutations of the parallel classes allowed are $(ab)(cd),\ (ac)(bd), (ad)(bc)$ and the identity. We have already calculated the elements of $GL_2(3)$ which act as $(ab), (ac)$ and (ad) on the parallel classes. By conjugation, we can calculate the other transpositions needed.

$$(cd) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix},\ (bd) = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix},\ (bc) = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}.$$

From this we can calculate matrices which induce the allowed permutations on the parallel classes. These along with their scalar multiples form the group S^*.

$$S^* = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

The group S is the group generated by the 8 matrices above along with the set T of translations in $AGL_2(3)$. In other words

$$S = \{\ t_{a,v} \mid t_{a,v}(u) = ua + v,\ u \in S^*,\ v \in T\}.$$

Now we show that S is sharply 2-transitive.
The stabiliser in S of an ordered pair of points in $AG_2(3)$ is the identity. No translation in T keeps this pair $P = (x_1, x_2)$ invariant therefore any element in S_P must lie in $GL_2(3)$. If we keep P invariant, then we must keep the line l that P is on invariant. From the nature of S, we must therefore keep the whole parallel class of l invariant. However there is only element of S which keeps one class invariant, and that is the identity.

As $T \cong \mathbb{F}_3^2$ and $|\mathbb{F}_2^3| = 3^2$ (3 choices for first entry of the vector and 3 for the second too), $|T| = 9$. Therefore $|S| = 8 \cdot 9 = 72$. Let Ω be the points of $AG_2(3)$. By Theorem 2.19, $|\Omega^{(2)}| = 9 \cdot 8 = 72$. Therefore we now know that $|S| = |\Omega^{(2)}|$ and that $|S_{(x_1,x_2)}| = 1$, and so by Theorem 2.25, S is sharply 2-transitive on Ω.

□

Theorem 4.37. *Aut*(W_{10}) *is 3-transitive on the set of points of* W_{10}.

Proof. The group H is sharply 2-transitive on the points of $AG_2(3)$ by Lemma 4.36, therefore H is 2-transitive on the points of $AG_2(3)$ by Theorem 2.24. The group H can be identified with $(\mathrm{Aut}(W_{10}))_\alpha$, therefore $(\mathrm{Aut}(W_{10}))_\alpha$ is 2-transitive on the points of W_α. This means that by Corollary 2.22 $\mathrm{Aut}(W_{10})$ is 3-transitive on the set of points of W_{10}.

□

5 Chapter 5

5.1 The construction of M_{11}

In this subsection we are going to construct a one point extension of $S(3,4,10)$. This will be an $S(4,5,11)$ Steiner system. We are also going to prove that any $S(4,5,11)$ Steiner system is unique up to isomorphism. We do this as $M_{11} := \mathrm{Aut}(S(4,5,11))$. We then prove several properties of M_{11}. This subsection follows the same construction of M_{11} as in [3].

Theorem 5.1. *If there exists $S(4,5,11)$ Steiner system, then it is unique up to isomorphism.*

Proof. This proof follows that of [3].

First we assume we have an $S(4,5,11)$ Steiner system and call it W. If we contract W by any point $\alpha \in W$, we create an $S(3,4,10)$ Steiner system by Theorem 3.12. In the same way, if we contract W by any other point $\beta \in W$, we create an S(3,4,10) Steiner system. Since $S(3,4,10)$ is unique up to isomorphism by Theorem 4.34, the contraction due to α and the contraction due to β are isomorphic. Thus we can say that the points of W consist of the points in $AG_2(3)$ as well as α and β.

The blocks containing α and β must be of the following form:

- $\Lambda \cup \{\alpha, \beta\}$ where Λ is a line of $AG_2(3)$;
- $\Xi \cup \{\alpha\}$ where Ξ is a quadrangle of Z_1;
- $\Xi \cup \{\beta\}$ where Ξ is a quadrangle of Z_2;

(where Z_1 and Z_2 are sets of quadrangles of the type defined in the last section - these subscripts are not important as long as they are distinct).

Otherwise, when we contract W by α or β or both, we do not get W_{10} and $AG_2(3)$ when we are supposed to.

Now we must describe the blocks of W which contain neither α nor β (and so are contained in $AG_2(3)$. We know that any set of 5 points in $AG_2(3)$ must contain a quadrangle by Theorem 4.15 and so each of the remaining blocks must contain a quadrangle from Z_3 (all sets of 4 must be covered by blocks exactly once the quadrangles in Z_3 have not been 'covered' yet). On the other hand, since each set of 4 points lie in exactly one blocks, none of these are from Z_1 or Z_2 as they are already 'covered'. This means that by Theorem 4.24(iii), each of the blocks of W disjoint from $\{\alpha, \beta\}$ has the form $\Xi \cup \{\delta\}$ where $\Xi \in Z_3$ and δ is the diagonal point of Ξ. This is because δ is the unique point of $AG_2(3)$ that ensures that there are no quadrangles in $\Xi \cup \{\delta\}$ that aren't in Z_3. □

We now prove the existence of an $S(4,5,11)$ Steiner system by constructing one. Let $\Omega = AG_2(3) \cup \{\alpha, \beta\}$ (where α and β are new points not in $AG_2(3)$). Define the set $\mathcal{B}$ of sets to consist of all sets of form:

- $B_1 := \Lambda \cup \{\alpha, \beta\}$ where Λ is a line of $AG_2(3)$;
- $B_2 := \Xi \cup \{\alpha\}$ where Ξ is a quadrangle of Z_1;
- $B_3 := \Xi \cup \{\beta\}$ where Ξ is a quadrangle of Z_2;
- $B_4 := \Xi \cup \{\delta\}$ where $\Xi \in Z_3$ and δ is the diagonal point of Ξ.

(where Z_1, Z_2 and Z_3 are sets of quadrangles of the type defined in the last section).

Note that any set of any of these types has size 5.
We must show that $\mathcal{B}$ is a set of blocks for an $S(4,5,11)$ Steiner system. To do this we must show that each set of 4 points in Ω lies in exactly one set of $\mathcal{B}$.

In anticipation of the result we will call the sets of type B_1, B_2, B_3, B_4, blocks.

Lemma 5.2. *If all sets of size 4 lie in at least one block of W each, then each set lies in exactly one block of W.*

Proof. There are exactly 18 blocks of each type B_2, B_3 and B_4 and12 of type B_1, so $|\mathcal{B}| = 66$.

$\binom{11}{4}/\binom{5}{4} = 66 = |\mathcal{B}|$ and so each set of 4 has to be in at most one block.

Therefore if every set of size 4 is in at least one block and at most one block, it is in one block. □

Due to Lemma 5.2, we only need to show that each set of size 4 in Ω lies in at least one block of type B_i where $1 \leq i \leq 4$. We begin with the sets of 4 which contain the new elements of Ω, namely α and β.

Lemma 5.3. *Each set of size 4 in Ω which contains α or β (or both) lies in at least one of the blocks in $\mathcal{B}$, namely one of type B_1, B_2, B_3.*

Proof. Now we will prove that each set of size 4 in Ω which contains α or β (or both) lies in one of these blocks.

Consider $U = \{x_1, x_2, x_3, \alpha\}$ where $x_1, x_2, x_3 \in AG_2(3)$. We know that $\{x_1, x_2, x_3\}$ is either a line or triangle in $AG_2(3)$. If $\{x_1, x_2, x_3\}$ is a line of $AG_2(3)$ then U lies in a block of the form B_1 where $\Lambda = \{x_1, x_2, x_3\}$.

If $\{x_1, x_2, x_3\}$ is a triangle then U lies in a block of the form B_2 as every triangle of $AG_2(3)$ lies in a unique quadrangle of Z_1 by Theorem 4.30.

In a similar way, a set of the form $\{x_1, x_2, x_3, \beta\}$ where $x_1, x_2, x_3 \in AG_2(3)$ lies in one of the blocks listed above.

Now we consider a set $V = \{x_1, x_2, \alpha, \beta\}$ where $x_1, x_2 \in AG_2(3)$. Any 2 points of $AG_2(3)$ lie in exactly one line of $AG_2(3)$ and therefore V lies in a of form B_1.

There are no more sets of size 4 in Ω that contain at least one of α and β so we are done. □

Lemma 5.4. *Consider any quadrangle Ξ in $AG_2(3)$. There is exactly one pair of lines in Ξ which are not parallel and do not intersect within Ξ. These two lines intersect outside of Ξ at the diagonal point of Ξ.*

Proof. This is clear to see from Figure 6 and Theorem 4.24, and the fact that $AGL_2(3)$ is transitive on quadrangles. □

Lemma 5.5. *Any set of size 4 which contains neither α nor β lies in at least one of the blocks in $\mathcal{B}$, namely one of form B_2, B_3, B_4.*

Proof. This proof follows that of [3].

Consider a set $U = \{x_1, x_2, x_3, x_4\}$ where $U \subseteq AG_2(3)$. If U is a quadrangle (as in in contains no 3 collinear points) then it must lie in exactly one of Z_1, Z_2 or Z_3 as it U cannot be of more than one type. This means U will lie in exactly one of the blocks, either of form B_2, B_3 or B_4 depending on which Z_i U lies in.

If U is not a quadrangle (so it contains at least one line) U must contain exactly one line Λ. This is because U contains 4 points but a line contains 3, so if there were 2 lines in U, the 2 lines must share 2 points, making them the same line. This logic also works for more than 2 lines in U. It remains to prove that U lies in a block of form B_4.

Without loss of generality, assume that Z_3 corresponds to the partition $ad \mid cb$ and that Λ lies in parallel class a. Call the point in $U \backslash \Lambda$, π. There are 3 lines through π which intersect with Λ (one of the 4 lines through π is parallel to Λ), one of of each class b, c and d. We choose the line of class d, call it Λ^* and name the third point on ρ. This point ρ is not on Λ otherwise the intersection point of Λ and Λ^*, say γ, and ρ would both be on Λ and Λ^* but each pair of points lies on a unique line. This is shown in Figure 8. We note that $\Lambda^* \subseteq U \cup \{\rho\}$. Let Ξ be the complement of $\{\gamma\}$ (the point of intersection of Λ and Λ^*) in $U \cup \{\rho\}$.

The set of four points Ξ is a quadrangle. Say $\Xi = \{x_1, x_2, \rho, \pi\}$, then x_1 and x_2 do not form a line together with any of the other 2 points Ξ in as they lies on a unique line with γ. The same goes for π and ρ. Therefore there are no 3 collinear points in Ξ. There are 2 lines in Ξ which don't intersect within Ξ but but are not parallel by Lemma 5.4. These lines are Λ and Λ^* as they intersect at $\gamma \notin \Xi$. These are of type a and d respectively and so Ξ is a $\{b, c\}$ quadrangle and γ is the diagonal point of Ξ. This means that $U \cup \{\rho\} = \Xi \cup \{\gamma\}$ is a block of form B_4 containing U. □

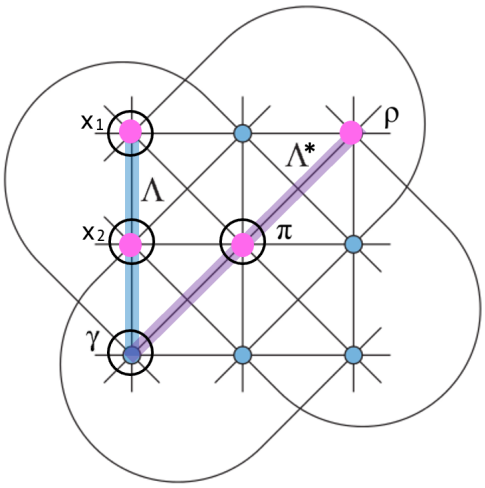

Figure 8

Theorem 5.6. *There exists an $S(4,5,11)$ Steiner system and it is unique up to isomorphism. We will call it W_{11}.*

Proof. The set $W = \{\Omega, \mathcal{B}\}$, as described above, is an $S(4,5,11)$ Steiner system. Therefore there exists an $S(4,5,11)$, and by Theorem 5.1, W is unique up to isomorphism, □

We now move onto the automorphism group of W_{11} which is called M_{11}. This is one of the groups we aimed to construct. We shall prove that M_{11} is sharply 4-transitive on the set of points of W_{11} and that M_{11} has order $11 \cdot 10 \cdot 9 \cdot 8$.

Theorem 5.7. *$M_{11} := Aut(W_{11})$ is sharply 4-transitive on the set of points of W_{11} and has order $11 \cdot 10 \cdot 9 \cdot 8$.*

Proof. The Steiner system W_{11} is a one-point extension of W_{10}, and W_{10} is uniquely determined up to isomorphism, and there is a unique way of choosing the blocks of W_{10} up to the action of $\mathrm{Aut}(W_{10})$ as proved in the previous section. Therefore M_{11} is transitive on the points of W_{11} by Theorem 3.15.

As M_{11} is transitive on Ω, all of the point stabilisers of M_{11} are isomorphic. Therefore we can now focus on $(M_{11})_\alpha$ where $\alpha \in \Omega$ without loss of generality.

By Theorem 3.13 we know that $(M_{11})_\alpha \subseteq \mathrm{Aut}(W_{10})$. As α is fixed by $(M_{11})_\alpha$, this means that blocks of type B_1 and B_2 can only be mapped to blocks of type B_1 and B_2 by elements of $(M_{11})_\alpha$ as they are the only blocks containing α. Plus as any block of type $B_1 \backslash \{\alpha\}$ is a quadrangles of $AG_2(3)$ and any block of type $B_2 \backslash \{\alpha\}$ is a line and a point of $AG_2(3)$ this means that any element of $(M_{11})_\alpha$ can only map a block of type B_i

to a block of type B_i ($i \in \{1,2\}$). This is because automorphism preserves structure. The blocks of type $B_1\backslash\{\alpha\}$ and $B_2\backslash\{\alpha\}$ are exactly the blocks of W_{10} therefore $(M_{11})_\alpha$ contains all automorphisms of $\mathrm{Aut}(W_{10})$. So we get $\mathrm{Aut}(W_{10}) \subseteq (M_{11})_\alpha$. Therefore $\mathrm{Aut}(W_{10}) = (M_{11})_\alpha$.

By Theorem 4.35 we know that $\mathrm{Aut}(W_{10})$ is transitive on the points of W_{10}, therefore so is $(M_{11})_\alpha$. Therefore by the fact that M_{11} is transitive on Ω and Corollary 2.22, we now know that M_{11} is 2-transitive on Ω.

Now we focus on $(M_{11})_{(\alpha,\beta)}$ where $(\alpha,\beta) \in \Omega^{(2)}$. We can choose these two points without loss of generality as M_{11} is 2-transitive on Ω. We already know that $(M_{11})_{(\alpha,\beta)}$ leaves invariant both of the blocks B_1 and B_2, therefore also leaves invariant Z_1. The group $(M_{11})_{(\alpha,\beta)}$ stabilises β, therefore blocks of type B_3 can only be mapped among themselves. This is because like before the only other option is a block of type B_1 as this is the only other type of block which contains β, but automorphims preserve structure and so this is not possible. Therefore $(M_{11})_{(\alpha,\beta)}$ leaves invariant Z_2. The quadrangles of Z_3 now have nowhere to be mapped to but to other quadrangles of Z_3 which means that $(M_{11})_{(\alpha,\beta)}$ stabilises all the partitions $ab|cd$, $ac|bd$ and $ad|bc$ in $AG_2(3)$. As $(M_{11})_{(\alpha,\beta)}$ is all such automorphims which stabilise all the partitions $ab|cd$, $ac|bd$ and $ad|bc$ in $AG_2(3)$, the group $(M_{11})_{(\alpha,\beta)}$ can be identified with S from Lemma 4.36. Therefore $(M_{11})_{(\alpha,\beta)}$ is sharply 2-transitive on $\Omega\backslash\{\alpha,\beta\}$.

Because of this and the fact that M_{11} is 2-transitive on Ω, we know by Corollary 2.26 that M_{11} is sharply 4-transitive on Ω.

By Corollary 2.28 where $n = 11$ and $k = 4$

$$|M_{11}| = |\{\alpha,\beta\}^{M_{11}}| \cdot |(M_{11})_{\{\alpha\beta\}}| = 11 \cdot 10 \cdot 9 \cdot 8.$$

□

5.2 The construction of M_{12}

In this subsection we are going to construct a one point extension of $S(4,5,11)$. This will be an $S(5,6,12)$ Steiner system. We are also going to prove that any $S(5,6,12)$ Steiner system is unique up to isomorphism. We do this as $M_{12} := \mathrm{Aut}(S(5,6,12))$. We then prove several properties of M_{12}. This subsection follows the same construction of M_{12} as in [3].

We are first going to prove that if an $S(5,6,12)$ Steiner system exists, then it is unique up to isomorphism. In order to do this we first assume we have an $S(5,6,12)$ Steiner system and call it W. If we contract W by any point α, β or $\gamma \in W$, we create an $S(4,5,11)$ Steiner system by Theorem 3.12. Since $S(4,5,11)$ is unique up to isomorphism by Theorem 5.6, the contraction due to α, β and γ respectively are

isomorphic. Thus we can say that the points of W consist of the points in $AG_2(3)$ as well as α, β and γ.

In order to describe the blocks of W, we must construct the set $\mathcal{C}_i$ (for $i \in \{1, 2, 3\}$) consisting of all the subsets of $AG_2(3)$ of the form $\Xi \cup \{\delta\}$ where $\Xi \in Z_i$ and δ is the diagonal point of Ξ.

The blocks of W containing α, β and γ are of the following form:

- $B_1 := \Lambda \cup \{\alpha, \beta, \gamma\}$ where Λ is a line of $AG_2(3)$;
- $B_2 := \Xi \cup \{\beta, \gamma\}$ where Ξ is a quadrangle in Z_1;
- $B_3 := \Xi \cup \{\alpha, \gamma\}$ where Ξ is a quadrangle in Z_2;
- $B_4 := \Xi \cup \{\alpha, \beta\}$ where Ξ is a quadrangle in Z_2;
- $B_5 := R \cup \{\alpha\}$ where R is in $\mathcal{C}_1$;
- $B_6 := R \cup \{\beta\}$ where R is in $\mathcal{C}_2$;
- $B_7 := R \cup \{\gamma\}$ where R is in $\mathcal{C}_3$.

This is because otherwise, when we contract W by α, β, γ or any combination of the 3, we do not get W_{11}, W_{10} and $AG_2(3)$ when we are supposed to.

Lemma 5.8. *There exists at least one set of 5 points in $AG_2(3)$ which does not contain a quadrangle along with its diagonal point.*

Proof. The set of five points $F =$ 00 10 01 11 12 contains 3 quadrangles (can test by trial and error, only $\binom{5}{4} = 5$ sets of 4 to test). The quadrangles are 00 10 01 11, 00 01 11 12 and 00 10 01 12 and their corresponding diagonal points are 22, 21 and 20 respectively. None of the diagonal points are in F. □

Lemma 5.9. *Let F be a set of 5 points in $AG_2(3)$ which does not contain any quadrangle Ξ with the diagonal point δ of Ξ. Then there is only one point γ in $AG_2(3)$ such that $F \cup \{\gamma\}$ contains no quadrangles along with their diagonal point. This new 6-set, $F \cup \{\gamma\}$, is the union of two distinct parallel lines in $AG_2(3)$.*

Proof. Due to the transitivity of $AGL_2(3)$ on quadrangles of $AG_2(3)$, we only need to prove this for one set of 5 points F. Let $F =$ 00 10 01 11 12. As shown in Lemma 5.8 we cannot choose 22, 21 or 20 for our 6th point γ. This forces us to choose 02. We can then show that no quadrangle of $F \cup \{02\}$ which includes 02 has a diagonal point in F. We can easily see that $F \cup \{02\}$ is the union of two distinct parallel lines in $AG_2(3)$. □

Lemma 5.10. *Let W be an $S(5,6,12)$ Steiner system with blocks containing those of types $B_1, \ldots, B_7$. Then the remaining blocks, i.e. the blocks of W disjoint from $\{\alpha, \beta, \gamma\}$, are of the form:*

- B_8 := *a union of two distinct parallel lines in $AG_2(3)$.*

Proof. Any set of 6 points of $W \backslash \{\alpha, \beta, \gamma\}$, i.e. $AG_2(3)$, contains 6 sets of 5 points which each contain at least one quadrangle, so each of the remaining blocks must contain a quadrangle along with a point. On the other hand, the 'extra' points cannot be cannot be the diagonal points of the quadrangles as these sets of 5 are already covered by the blocks of the form B_5, B_6 and B_7. So we are looking for a 6 point set which contains no quadrangles along with their diagonal point. By Lemma 5.9, this is a union of two distinct parallel lines in $AG_2(3)$. □

Theorem 5.11. *If there exists an $S(5,6,12)$ Steiner system, then it is unique up to isomorphism.*

Proof. If there does exists an $S(5,6,12)$ Steiner system, we have proved above that there is only one of them up to isomorphism. □

We now prove the existence of an $S(5,6,12)$ Steiner system by proving that the construction we have just made does indeed work. Let $\Omega = AG_2(3) \cup \{\alpha, \beta, \gamma\}$ (where α, β and γ are new points not in $AG_2(3)$). Define the set $\mathcal{B}$ of sets to consist of all sets of form B_i where $1 \leq i \leq 8$.

Note that any set of any of these types has size 6.
We must show that $\mathcal{B}$ is a set of blocks for an $S(5,6,12)$ Steiner system. To do this we must show that each set of 5 points in Ω lies in exactly one set of $\mathcal{B}$.

In anticipation of the result we will call the sets of type B_i, blocks.

Lemma 5.12. *If all sets of size 5 in Ω lie in at least one block of $\mathcal{B}$ each, then each set lies in exactly one block of $\mathcal{B}$.*

Proof. There are exactly 12 blocks of type B_1, 18 of each type $B_2, \ldots, B_7$ and 12 of type B_8, so $|\mathcal{B}| = 132$.

$\binom{12}{5} / \binom{6}{5} = 132 = |\mathcal{B}|$ and so each set of 5 has to be in at most one block.

Therefore if every set of size 5 is in at least one block and at most one block, it is in one block. □

Lemma 5.13. *Any set of 5 points of Ω which includes any nonempty subset of $\{\alpha, \beta, \gamma\}$ lies in at least one block of type B_i where $1 \leq i \leq 7$.*

Proof. The 5 types of 5-sets which contain α are:

1. α and a quadrangle in Z_i for $i \in \{1, 2, 3\}$;

2. α and a set of 4 points containing a line in $AG_2(3)$;

3. α, β and a triangle in $AG_2(3)$;

4. α, β and a line in $AG_2(3)$;

5. α, β, γ and a pair of points in $AG_2(3)$.

We now prove that these sets are in at least one block of $\mathcal{B}$. Below we state which blocks each of the sets are in along with some explanation if this is needed.

1. B_3, B_4 or B_5 depending on the value of i in Z_i.

2. B_5 by the second half of the proof of Lemma 5.5.

3. B_4 as each triangle of $AG_2(3)$ is in a quadrangle from Z_3 by Theorem 4.30.

4. B_1.

5. These sets are in blocks of type of B_1 as every pair of points of $AG_2(3)$ is in a line of $AG_2(3)$.

We can use very similar logic to show that the 5-sets which contain β and those than contain γ are in at least one block of $\mathcal{B}$.

□

Lemma 5.14. *Any set of 5 points of Ω which is disjoint from $\{\alpha, \beta, \gamma\}$ lies in at least one block of type B_8.*

Proof. First we consider a set, F of 5 points in $\Omega \backslash \{\alpha, \beta, \gamma\}$, i.e. $AG_2(3)$. By Theorem 4.15 we know that F contains at least one quadrangle. We define the set of quadrangles in F to be $Q := \{\Xi_1, \ldots, \Xi_n\}$. If $F \backslash \Xi_i$ is ever the diagonal point of Ξ_i, then these 5 points are contained in a $\mathcal{C}_i$ and therefore in a block of the form B_5, B_6 or B_7. If $F \backslash \Xi_i$ is never the diagonal point of Ξ_i, then we must continue with our work. We want to pick a 6th point to add to F that will not be the diagonal point of any of the quadrangles Ξ_i. We pick one of the quadrangles in Q, say Ξ_1, and without loss of generality we assume Ξ_1 has type $\{a, b\}$. Call the point in $F \backslash \Xi_1$, γ. As we can see in Figure 6, γ lies on either a line of class a or b which makes up Ξ_1. If we assume without loss of generality that γ is on a line, l of Ξ_1 of class a then we can see that there is a point on the other line of class a which is in Ξ_1, call this point π. It is clear to see that π cannot be the diagonal point of Ξ_1 and that $F \cup \{\pi\}$ is a union of two distinct parallel lines which 'covers' F. This is shown in Figure 9. Therefore we know that each set of five points not covered by the blocks of type B_i where $1 \leq i \leq 7$ is covered by a block of type B_8. □

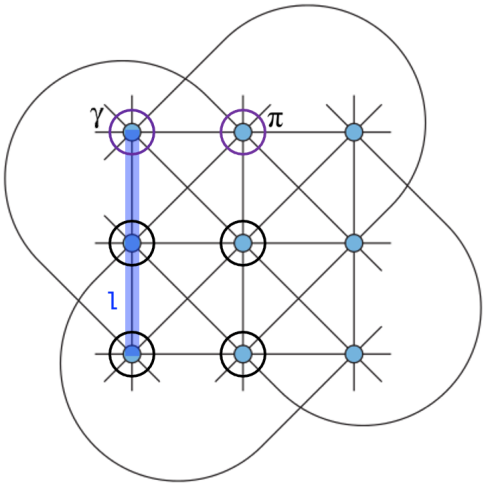

Figure 9

Theorem 5.15. *There exists an $S(5,6,12)$ Steiner system and it is unique up to isomorphism. We will call it W_{12}.*

Proof. The set $W = \{\Omega, \mathcal{B}\}$, as described above, is an $S(5,6,12)$ Steiner system and by Theorem 5.11, W is unique up to isomorphism. □

We now move onto the automorphism group of W_{12}, which is called M_{12}. This is second of the groups we aimed to construct. We shall prove that M_{12} is sharply 5-transitive on the set of points of W_{12} and that M_{12} has order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Theorem 5.16. *$M_{12} := Aut(W_{12})$ is sharply 5-transitive on the set of points of W_{12} and $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.*

Proof. The group W_{12} is a one-point extension of W_{11}, and W_{11} is uniquely determined up to isomorphism, and there is a unique way of choosing the blocks of W_{11} up to the action of $\mathrm{Aut}(W_{11})$ as proved in the previous section. Therefore M_{12} is transitive on the points of W_{12} by Theorem 3.15.

As M_{12} is transitive on Ω, all of the point stabilisers of M_{12} are isomorphic. Therefore we can now focus on $(M_{12})_\gamma$ where $\gamma \in \Omega$ without loss of generality.

We know that $(M_{12})_\gamma \subseteq M_{11}$ by Theorem 3.13. The group $(M_{12})_\gamma$ is the group of all automorphisms which leave the blocks of type B_1, B_2, B_3 and B_7 invariant. It is clear to see that if we remove γ from each of these blocks that we get all the blocks of W_{11}. Therefore $M_{11} \subseteq (M_{12})_\gamma$. From this we know that $M_{11} = (M_{12})_\gamma$

We know by Theorem 5.7 that M_{11} is sharply 4-transitive on the elements of W_{11}, and that for any $\gamma \in W_{12}$, $(M_{12})_\gamma = M_{11}$. Therefore $(M_{12})_\gamma$ is sharply 4-transitive

on the elements of W_{11}. By Corollary 2.22 this proves that M_{12} is 5-transitive on the points of W_{12}. Then by Theorem 2.26, where $i = 1$ and $k = 5$, M_{12} is sharply 5-transitive on the points of W_{12}.

By the orbit stabiliser property (or by Corollary 2.28)

$$|M_{12}| = |\gamma^{M_{12}}||(M_{12})_\gamma| = |W_{12}||M_{11}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8.$$

□

5.3 Conclusion

We have now constructed the two smallest Mathieu groups M_{11} and M_{12} and proved certain of their properties, such as their order and their multiple transitivity. As stated in the introduction, both of these groups are simple and this is proved by [10] by using Sylow Theorems. One can also construct the larger Mathieu groups M_{22}, M_{23} and M_{24} using similar methods to those in this project however instead of starting with $AG_2(3)$ we start with the projective plane $PG_2(4)$. Given time, we would have discussed these groups, their order, their multiple-transitivity and their simplicity also. Some other properties that would have been interesting to prove are that some of these Mathieu groups are subgroups of others and some are not, i.e. $M_{12} \leqslant M_{24}$ but $M_{11} \not\leqslant M_{22}$. This is shown in [5] by investigating maximal subgroups. While we did not have time to look into these areas, we did achieve our aim of constructing the Steiner systems which are needed to construct M_{11} and M_{12}. We also showed that these Steiner systems are unique up to isomorphism and then proved certain properties of their automorphism groups.

6 References

[1] Aschbacher, M. (1980). The Classification of the Finite Simple Groups. The Mathematical Intelligencer, 3(2), 736–740. https://doi.org/10.1007/bf03022850

[2] Conrad, K. (2020). Generating Sets. https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf

[3] Dixon, J. D., & Mortimer, B. (1996). Permutation Groups (Graduate Texts in Mathematics, 163) (1996th ed.). Springer.

[4] Dummit, D. S., & Foote, R. M. (2003). Abstract Algebra, 3rd Edition (3rd ed.). Wiley.

[5] Garbe, D., & Mennicke, J. L. (1964). Some Remarks on the Mathieu Groups. Canadian Mathematical Bulletin, 7(2), 201–212. https://doi.org/10.4153/cmb-1964-018-3

[6] Malik, D. S., Mordeson, J. M., & Sen, M. K. (1996). Fundamentals of Abstract Algebra. McGraw-Hill College.

[7] Moorhouse, G. E. (2017). Incidence geometry. http://ericmoorhouse.org/handouts/Incidence_Geometry.pdf

[8] Rose, J. S. (2012). A Course on Group Theory (Dover Books on Mathematics) (1st ed.). Dover Publications.

[9] Rotman, J. J. (1994). An Introduction to the Theory of Groups (Graduate Texts in Mathematics, 148) (4th ed.). Springer.

[10] Rubinstein-Salzedo, S. (2011). Mathieu groups. http://simonrs.com/MathieuGroups.pdf

[11] Solomon, R. (2001). A brief history of the classification of the finite simple groups. Bulletin of the American Mathematical Society, 38(03), 315–353. https://doi.org/10.1090/s0273-0979-01-00909-0

[12] Wikipedia contributors. (2021, February 10). Sporadic group. Wikipedia. https://en.wikipedia.org/wiki/Sporadic_group