CONSTRUCTIONS AND SIMPLICITY OF THE MATHIEU GROUPS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
MATHEMATICS

By
Mete Han Karakaş
August 2020

CONSTRUCTIONS AND SIMPLICITY OF THE MATHIEU GROUPS

By Mete Han Karakaş

August 2020

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Matthew Justin Karcher Gelvin (Advisor)

Laurence John Barker

Ömer Küçüksakallı

Approved for the Graduate School of Engineering and Science:

Ezhan Karaşan
Director of the Graduate School

ABSTRACT

CONSTRUCTIONS AND SIMPLICITY OF THE MATHIEU GROUPS

Mete Han Karakaş
M.S. in Mathematics
Advisor: Matthew Justin Karcher Gelvin
August 2020

Of the 26 sporadic finite simple groups, 5 were discovered by E. Mathieu in 1861 and 1873 [1], [2]. These *Mathieu groups* are the focus of this thesis, where we will prove their simplicity using elementary methods. E. Witt [5] realized a connection between the Mathieu groups and certain combinatorial structures known as Steiner systems. We will follow his construction to define the Mathieu groups as the automorphism groups of certain Steiner systems. Much of the work of the thesis lies in the construction of these Steiner systems, which we achieve by using both methods from finite geometry and the theory of Golay codes.

Keywords: Mathieu groups, Steiner systems, Golay codes.

ÖZET

MATHIEU GRUPLARININ OLUŞTURULMASI VE BASİTLİĞİ

Mete Han Karakaş
Matematik, Yüksek Lisans
Tez Danışmanı: Matthew Justin Karcher Gelvin
Ağustos 2020

26 tane sporadik sonlu basit gruplardan 5 tanesi 1861 ve 1873 yıllarında E. Mathieu tarafından keşfedildi [1], [2]. Bu *Mathieu grupları* tezimizin odak noktası. Tezde bu grupların basitliğini elementer yollarla kanıtladık. E. Witt [5] Mathieu gruplarla kombinatorik bir yapı olan Steiner sistemler arasındaki bağlantıyı fark etti. Biz E. Witt'in grupları oluşturma yolunu takip ettik ve bu yüzden Mathieu grupları Steiner sistemlerin otomorfizması olarak tanımladık. Tezdeki çalışmanın büyük bölümü de bu Steiner sistemlerin oluşturulmasına dayanıyor. Oluşturma metodlarından ikisi sonlu geometriye, biri ise Golay kod teorisine dayanıyor.

Anahtar sözcükler: Mathieu grupları, Steiner sistemler, Golay kodları.

Year after year I have searched for myself,
In no way have I found myself.
Am I a spectre or am I a dream? It cannot be known.
In no way have I found myself.

Am I a human, an animal or a plant?
Am I a crop, sown and reaped,
Or else, am I health itself?
In no way have I found myself.

Aşık Veysel Şatıroğlu

Transl. by Ruth Davis

Special thanks to Yılmaz Akyıldız

çınla'mak...

Acknowledgement

As always, I will write my feelings.

Firstly I would like to thank my dearest advisor Matthew Gelvin. I am deeply indebted to Matthew Gelvin, who has been a constant source of support throughout my thesis study in Bilkent. Thanks to his enormous and endless patience, I have finished my master's degree at Bilkent in the first place. Being a student of him will always be my great honour and privilege. I truly learned how to act like a mathematician from him. He is simply my mathematical role-model. Dear Matthew Gelvin is also one of the kindest and the most generous person in my life. Thank you for everything that you have done for me, sir.

I would like to thank thesis jury members Laurence John Barker and Ömer Küçüksakallı for careful readings and detailed reviews of my thesis.

I have been very fortunate to be surrounded by great colleagues in Bilkent. I want to thank each one of them. Whenever I have sought help for departmental issues, Serkan Sonel has always been on my side. Also, I want to thank him for his enormous support throughout my study. The latex format of the thesis has been prepared by Anıl Tokmak and he has shown me how to type in latex. Thank you, Anıl. I have spent most of my free time with my dear colleagues Utku Okur, Yaman Paksoy, Melike Çakmak, and Sueda Kaycı. I want to thank Utku, Yaman, Melike, and Sueda for making my time enjoyable. I have already missed our conversations.

I would like to thank my dear friend Nurhan Güner. Even though she was in the USA at the time of my last year in master's, I always felt her warm support.

I would like to thank my dear friend Ayberk Sadıç. We have met each other since high school, and I also have been so fortunate to attend ODTÜ together with him for

our undergraduate degrees. I am very grateful for our long-time strong friendship.

I would like to thank my dear friend Tunahan Durmaz. His encouragement and great support were highly acknowledged during my study in masters.

My mother Gülüşan Ünal is always my greatest strength for my entire life. She is the strongest person I have ever seen. No matter what happens in life, my mother always finds a way to fight. I am very fortunate to be her son. I believe that I will be a dignified mathematician in the future and make my mother so proud.

Çınla Akdere, I am grateful for your existence and uniqueness in my life. I find life more beautiful with you. You have the warmest heart in which I always want to be. Thank you for everything.

Contents

This thesis is dedicated

to my mother Gülüşan Ünal, who is the greatest survivor in life,

to Çınla Akdere, who is the most amazing person in my life,

to the memory of my father Şükrü Karakaş (1956-2020),

to the memory of distinguished mathematician Cem Tezer (1955-2020),

and

to my advisor Matthew Gelvin, who is my mathematical role-model.

Chapter 1

Introduction

1.1 Motivation

Let G be a finite group. If G does not contain any non-trivial normal subgroup then G is called *finite simple group*. Emile Mathieu gave first examples of finite simple groups in his two articles published in 1861 and 1873 [1], [2]. Now the groups that he introduced are called the Mathieu groups.

For many years mathematicians have tried to determine all finite simple groups. In 1980's, the classification of finite simple groups has been completed [3]. Now the classification theorem is stated below.

Theorem 1.1.1. [4, **The Classification Theorem**]

Let G be a finite simple group. Then G is isomorphic to one of the following groups as follows:

(i) A cyclic group of prime order,

(*ii*) *An alternating group of degree n for* $n \geq 5$,

(*iii*) *A simple group of Lie type,*

(*iv*) *One of the twenty-six sporadic simple groups.*

The Mathieu groups are the five of the list of the twenty-six sporadic simple groups. In addition, these five groups are permutation groups that act multiply transitive on $11, 12, 22, 23$ and 24 points respectively and denoted by $M_{11}, M_{12}, M_{22}, M_{23}$ and M_{24}. In particular, M_{12} and M_{24} are 5-transitive, M_{22} is 3-transitive and also M_{11} and M_{23} are 4-transitive [8, Chapter 9].

Furthermore, Ernst Witt has showed the relation between combinatorial structures known as Steiner systems and the Mathieu groups in his article [5]. He defined the Mathieu groups as the automorphism groups of certain Steiner systems. Then we will follow his construction to define the Mathieu groups as the automorphism groups of certain Steiner systems. Then definitions of the Mathieu groups based on Steiner systems as follows [16, Chapter 6]:

(*i*) $M_{24} := Aut(S(5, 8, 24))$

(*ii*) $M_{23} := Aut(S(4, 7, 23))$

(*iii*) $M_{22} := Aut(S(3, 6, 22))$

(*iv*) $M_{12} := Aut(S(5, 6, 12))$

(*v*) $M_{11} := Aut(S(4, 5, 11))$

In history, there are several methods to construct the Mathieu groups. Since we define the Mathieu Groups as the automorphism group of Steiner systems, constructing the Mathieu groups is equivalent to constructing the associated Steiner system.

1.2 Main focus of the thesis

Our much of the work lies in the constructions of $S(5,6,12)$ and $S(5,8,24)$. We achieve our goal for the construction of $S(5,6,12)$ by using methods from finite geometry. Also we achieve our goal for construction of $S(5,8,24)$ by using the theory of Golay codes. Then we see that $S(4,7,23)$, $S(3,6,22)$ and $S(4,5,11)$ are the immediate results of the latter Steiner systems by Theorem 3.2.1.

We consider showing the simplicity of the Mathieu groups as a supplementary part of the thesis. We do not deeply study simplicity. We aim to show the simplicity of the Mathieu groups by using group-theoretic elementary methods. First we follow the first three sections in chapter 9 of the book [8] to develop simplicity criteria for M_{12}, M_{24} and M_{22} in chapter 2. Then we develop Theorem 7.2.1 for showing simplicity of M_{11} and M_{23} in chapter 7.

1.3 Outline of the thesis

We will briefly explain the contents of the thesis.

In chapter 2, we give some background knowledge on group theory and finite geometries. In particular, we review group actions, Sylow theorems and k-transitivity in group theory. We develop the criteria of simplicity for multiply transitive groups that are used in chapter 7.

Also we explain affine and projective planes in chapter 2 since some certain Steiner systems are exactly affine or projective planes. In particular, our constructions of $S(5,6,12)$ based on $S(2,3,9)$ and $S(2,4,13)$, and $S(2,3,9)$ is a finite affine plane and $S(2,4,13)$ is a finite projective plane.

In chapter 3, we introduce Steiner systems and their properties. We investigate the necessary and sufficient conditions of the existence of Steiner systems. Also we explore properties of the automorphisms of Steiner systems.

In chapter 4, we form $S(5, 6, 12)$ by using Steiner system of type $S(2, 4, 13)$, that is a projective plane, due to Hans Havlicek and Hanfried Lenz [19]. We classify sets containing six points on a projective plane and develop blocks of $S(5, 6, 12)$.

In chapter 5, we form $S(5, 6, 12)$ by using Steiner system of type $S(2, 3, 9)$, that is an affine plane. The construction is based on 3-fold extension of $S(2, 3, 9)$. In other words, we first show the existence of $S(3, 4, 10)$ and continue in this fashion. Finally, we show the existence of $S(5, 6, 12)$.

In chapter 6, we form the binary Golay code and $S(5, 8, 24)$ simultaneously. We realize that binary Golay code of 12 dimension with length 24 is exactly Steiner system of type $S(5, 8, 24)$.

In chapter 7, we show the simplicity of the Mathieu groups in an elementary way. We firstly develop our main Theorem 7.1.5. Also we use simplicity criteria that are introduced in chapter 2.

In conclusion, we show two different construction methods for $S(5, 6, 12)$. Also we show construction of the binary Golay code and $S(5, 8, 24)$.

Chapter 2

Preliminaries

In this chapter, we will give some background knowledge that we will use throughout the thesis.

2.1 Review of group theory

In this section, we follow several algebra books: [6], [7], [8], [9], [10], [11].

2.1.1 Permutation groups

We start with basic definitions regarding permutations.

Definition 2.1.1. Let X be a non-empty set. A *permutation* of X is a bijective function from X to X.

Definition 2.1.2. The set of all permutations of a set X is called the

permutation group or *symmetric group* on X. It is denoted by S_X. If X is the set of $\{1, 2, ..., n\}$, then we usually write S_n. The group structure on S_X is the composition of permutations.

Definition 2.1.3. Let π be in S_n and i be in $\{1, 2, ..., n\}$. π *fixes* i if $\pi(i) = i$. Also π *moves* i if $\pi(i) \neq i$.

Definition 2.1.4. Let $i_1, i_2, ..., i_r$ be distinct integers in $\{1, 2, ..., n\}$ and π be in S_n. If $\pi(i_1) = i_2, \pi(i_2) = i_3, \pi(i_3) = i_4, ..., \pi(i_{r-1}) = i_r, \pi(i_r) = i_1$ and π fixes the other integers (if any) then π is called an *r-cycle* or is a cycle of *length* r. A 2-*cycle* is called *transposition*.

Definition 2.1.5. Let π be an r-cycle. Then π will be denoted by $(i_1\ i_2\ ...\ i_r)$. Then r-cycle π can be seen as a clockwise rotation of a circle and so any i_j can be considered as a first point of a cycle. Thus we have r different cycle notations as follows:

$$(i_1\ i_2\ ...\ i_{r-1}\ i_r) = (i_2\ i_3\ ...\ i_r\ i_1) = ... = (i_r\ i_1\ ...\ i_{r-2}\ i_{r-1}).$$

Definition 2.1.6. Let α, λ be in S_n. Then α and λ are *conjugate* if there is a permutation γ such that $\gamma\alpha\gamma^{-1} = \lambda$.

Now, we are ready to prove our next theorem.

Theorem 2.1.7. *Let $\pi = (i_1\ i_2\ ...\ i_{l-1}\ i_l)$ be l-cycle in S_n. For all $\alpha \in S_n$,*

$$\alpha\pi\alpha^{-1} = (\alpha(i_1)\ \alpha(i_2)\ ...\ \alpha(i_l)).$$

Proof. Let $X = \{1, 2, ..., n\}$ and S_n be the set of all permutations of X. Since $\alpha \in S_n$, α is a bijection from X to X. This means that $\alpha(1), \alpha(2), ..., \alpha(n)$ are all distinct. Therefore we can write X as a set of $\{\alpha(1), \alpha(2), ..., \alpha(n)\}$. Let r be any integer such that $1 \leq r < l$. Then $\alpha(i_r) \in X$. Hence $\alpha\pi\alpha^{-1}(\alpha(i_r)) = \alpha(\pi(\alpha^{-1}(\alpha(i_r)) = \alpha(\pi(i_r)) = \alpha(i_{r+1})$. Moreover when $r = l$, $\alpha\pi\alpha^{-1}(\alpha(i_l)) = \alpha(\pi(\alpha^{-1}(\alpha(i_l)) = \alpha(\pi(i_l)) = \alpha(i_1)$.

Now let $x \in X$ such that $x \neq \alpha(i_r)$ for all r, where $1 \leq r \leq l$. Also $\alpha^{-1}(x) \in X$ and $\alpha^{-1}(x) \neq i_r$ for all r, where $1 \leq r \leq l$. Hence $\alpha\pi\alpha^{-1}(x) = \alpha(\pi(\alpha^{-1}(x)) = \alpha(\alpha^{-1}(x)) = x$. Therefore we have $\alpha\pi\alpha^{-1} = (\alpha(i_1)\ \alpha(i_2)\ ...\ \alpha(i_l))$. □

2.1.2 Group actions

In our discussion, a group G will be finite and a set X will be non-empty. In this section, we will develop relation between orbits and stabilisers of the group action and their special cases.

Definition 2.1.8. Let G be a group and X be a set. A $(left)$ *group action* of G on X is a function $\mu : G \times X \longmapsto X$ that satisfies the following properties:

(1) $1x = x$ for all $x \in X$.

(2) $g_1(g_2x) = (g_1g_2)x$ for all $x \in X$ and $g_1, g_2 \in G$.

Then we will say that G acts on X and call X a *G-set*.

Example 2.1.9. Let G be $\mathbb{Z}_2 = \{1, \alpha\}$ and X be $\mathbb{R}_2 = \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{R}\}$. We will define the action of the element α on X in this way: $\alpha(x_1, x_2) = (-x_1, -x_2)$. The first property of a group action is satisfied trivially. The second property of a group action is satisfied as follows; $1(\alpha(x_1, x_2)) = 1(-x_1, -x_2) = (-x_1, -x_2)$. Also, $(1\alpha)(x_1, x_2) = \alpha(x_1, x_2) = (-x_1, -x_2)$. Therefore G acts on X.

Theorem 2.1.10. *Let G act on X, where G is a group and X is a non-empty set. Define a relation $\sim$ on X by for all x,$y \in X$, $x \sim y$ if and only if $gx = y$ for some $g \in G$. Then $\sim$ is an equivalence relation on X.*

Proof. Since $1x = x$ for all $x \in X$, we have $x \sim x$. Hence $\sim$ is reflexive. Let x, y, z be in X. Now we suppose that $x \sim y$. Then there exists $g \in G$ such that $gx = y$. It

follows that $x = g^{-1}(gx) = g^{-1}y$. We see that $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = 1x = x$. Hence $y \sim x$ and $\sim$ is symmetric. Lastly, we suppose that $x \sim y$ and $y \sim z$. Then there exist $g_1, g_2 \in G$ such that $g_1x = y$ and $g_2y = z$. Thus $(g_2g_1)x = g_2(g_1x) = g_2y = z$. Hence $x \sim z$ and so $\sim$ is transitive. Therefore $\sim$ is an equivalence relation on X. □

Definition 2.1.11. Let G act on X, where G is a group and X is a non-empty set. The equivalence classes $Gx = \{gx : g \in G\}$ determined by the equivalence relation in Theorem 2.1.10 are called the *orbits* of G on X. The orbit containing $x \in X$ is denoted by $\mathcal{O}(x)$.

Lemma 2.1.12. *Let G act on X, where G is a group and X is a non-empty set. For all $x \in X$, the subset $G_x = \{g \in G : gx = x\}$ is a subgroup of G.*

Proof. Let $x \in X$. $1 \in G_x$ since $1x = x$. Hence $G \neq \varnothing$. Let g_1, g_2 be in G_x. Then we have $g_1x = x$ and $g_2x = x$. It follows that $g_2^{-1}(g_2x) = (g_2^{-1}g_2)x = x = g_2^{-1}x$. This means $g_2^{-1} \in G_x$. Moreover $(g_2^{-1}g_1)x = g_2^{-1}(g_1x) = g_2^{-1}x = x$. Hence $g_2^{-1}g_1 \in G_x$. Therefore G_x is a subgroup of G. □

Definition 2.1.13. The subgroup G_x of Lemma 2.1.12 is called *stabiliser* of x.

We have defined the orbit and the stabiliser of a group action so far. We want to prove the Orbit-Stabiliser Theorem in our following discussion. For this purpose, we define cosets of subgroup of a group G and show their main properties.

Definition 2.1.14. Let H be a subgroup of G. The set $gH = \{gh : h \in H\}$ is called $(left)$ *coset* of H in G for all $g \in G$.

Theorem 2.1.15. *Let H be a subgroup of G. Either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$ for all $g_1, g_2 \in G$.*

Proof. Let $g_1, g_2 \in G$, and suppose that $g_1H \cap g_2H \neq \emptyset$. Hence there exists $x \in G$ such that $x \in g_1H \cap g_2H$. This means that $x \in g_1H$ and $x \in g_2H$ and so $x = g_1h_1$

and $x = g_2h_2$ for some $h_1, h_2 \in H$. Since $g_1h_1 = g_2h_2$, $g_2^{-1}g_1 = h_2h_1^{-1} \in H$. Therefore $g_1H = g_2H$. □

Corollary 2.1.15.1. *The set of cosets $\{gH : g \in G\}$ forms a partition of G.*

Proof. Straightforward from the previous theorem. □

Theorem 2.1.16. *Let H be a subgroup of G. Then there is a bijection between H and gH for all $g \in G$.*

Proof. Let $g \in G$. We will show the existence of a bijection between H and its left coset gH. Define a map $\gamma : H \longmapsto gH$ by $\gamma(h) = gh$ for all $h \in H$. For any $h_1, h_2 \in H$, $\gamma(h_1) = \gamma(h_2)$ if and only if $gh_1 = gh_2$. Thus γ is well-defined and one-to-one. Let $gh \in gH$. Since $h \in H$, $\gamma(h) = gh$. Hence γ is onto. Therefore γ is a bijection map and $|H| = |gH|$. □

Definition 2.1.17. Let H be a subgroup of G. The number of distinct left cosets of H in G is denoted by $[G : H]$ and is called the *index* of H in G.

Now, we are ready to prove our main theorem in this section.

Theorem 2.1.18. Orbit-Stabiliser Theorem[6] *Let G act on X, where G is a group and X is a non-empty set. For all $x \in X$,*

$$|\mathcal{O}(x)| = [G : G_x].$$

Proof. Let $x \in X$. We will show the existence of a bijection between left cosets of G_x and $\mathcal{O}(x)$. Define a map $\alpha : G/G_x \longmapsto \mathcal{O}(x)$ by $\alpha(gG_x) = gx$ for all $gG_x \in G/G_x$.

We first look at well-definedness of the map. We suppose that $g_1G_x = g_2G_x$ for some $g_1, g_2 \in G$. Then we get $g_2^{-1}g_1 \in G_x$, and so $g_2^{-1}g_1x = x$. It follows that $g_2g_2^{-1}g_1x = g_2x$. Hence this means $g_1x = g_2x$, and α is well-defined.

Secondly, we suppose that $\alpha(g_1G_x) = \alpha(g_2G_x)$ for some $g_1, g_2 \in G$. Thus we have $g_1x = g_2x$. It follows that $g_2^{-1}g_1x = x$, and so $g_2^{-1}g_1 \in G_x$. Therefore we get $g_1G_x = g_2G_x$, and α is one-to-one.

Lastly, let $y \in \mathcal{O}(x)$. Then there exists $g_3 \in G$ such that $g_3x = y$. Hence $\alpha(g_3G_x) = g_3x = y$, and so α is onto. Therefore α is a bijection map, and so $|\mathcal{O}(x)| = [G : G_x]$. □

Example 2.1.19. Let G be a group. We will define an action of G on itself by conjugation: $\beta : G \times G \longmapsto G$ by $\beta(gx) = gxg^{-1}$ for all $g, x \in G$. We check two properties of a group action. Let $g_1, g_2, x \in G$. Firstly, $1x = 1x1 = x$. Secondly, $g_1(g_2x) = g_1(g_2xg_2^{-1}) = g_1g_2xg_2^{-1}g_1^{-1} = (g_1g_2)x$. Hence this action satisfies group action criteria. Now we will find out orbit and stabiliser of it.

Then the orbit $\mathcal{O}(x) = \{gx : g \in G\} = \{gxg^{-1} : g \in G\}$ for all $x \in G$. The stabiliser $G_x = \{g \in G : gx = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$ for all $x \in G$.

Example 2.1.20. [9] Let G be a group. We will define an action of G on the set of all subsets of G, namely $\mathcal{P}(G)$, : $\delta : G \times \mathcal{P}(G) \longmapsto \mathcal{P}(G)$ by $\delta(gA) = gAg^{-1}$ for all $g \in G$ and $A \in \mathcal{P}(G)$. We check two properties of a group action. Let $g_1, g_2 \in G$ and $A \in \mathcal{P}(G)$. Firstly, $1A = 1A1 = A$. Secondly, $g_1(g_2A) = g_1(g_2Ag_2^{-1}) = g_1g_2Ag_2^{-1}g_1^{-1} = (g_1g_2)A$. Hence this action satisfies group action criteria. Now we will find out orbit and stabiliser of it.

Then the orbit $\mathcal{O}(A) = \{gA : g \in G\} = \{gAg^{-1} : g \in G\}$ for all $A \in \mathcal{P}(G)$. The stabiliser $G_A = \{g \in G : gA = A\} = \{g \in G : gAg^{-1} = A\} = \{g \in G : gA = Ag\}$ for all $A \in \mathcal{P}(G)$.

Definition 2.1.21. (i) The orbit $\mathcal{O}(x)$ of Example 2.1.19 is called the *conjugacy class* of x in G.

(ii) The stabiliser G_x of Example 2.1.19 is called the *centralizer* of x in G and is

denoted by $C_G(x)$.

(*iii*) Two subsets A and B are called *conjugate* in G if there exists $g \in G$ such that $B = gAg^{-1}$.

(*iv*) The stabiliser G_A of Example 2.1.20 is called the *normalizer* of A in G and is denoted by $N_G(A)$.

The next two propositions are the special cases of the Orbit-Stabiliser Theorem.

Proposition 2.1.22. *Let G act on itself by conjugation. Then the number of conjugates of x is the index of its centralizer. That is,*

$$|\mathcal{O}(x)| = [G : C_G(x)] \ for\ all\ x \in G.$$

Proposition 2.1.23. *Let G act on $\mathcal{P}(G)$ by conjugation. Then the number of conjugates of A is the index of its normalizer. That is,*

$$|\mathcal{O}(A)| = [G : N_G(A)] \ for\ all\ A \in \mathcal{P}(G).$$

Definition 2.1.24. Let G act on X, where G is a group and X is a non-empty set. Let $x \in X$ and $g \in G$. Then x is called $fixed$ by g if $gx = x$. If $gx = x$ for all $g \in G$ then x is called $fixed$ by G.

Theorem 2.1.25. *Let G act on X, where G is a group and X is a non-empty set. For all $g \in G$ and $x \in X$, $\rho_g : x \longmapsto gx$ is a permutation of X. Then $\rho : G \longmapsto S_X$ defined by $\rho(g) = \rho_g$ is a homomorphism.*

Proof. Firstly, we will show that ρ_g is a permutation of X. Let $g \in G$ and $x \in X$. Then, $\rho_g\rho_{g^{-1}}(x) = \rho_g(g^{-1}x) = gg^{-1}x = x$. Also $\rho_{g^{-1}}\rho_g(x) = \rho_{g^{-1}}(gx) = g^{-1}gx = x$. Hence ρ_g has an inverse $\rho_{g^{-1}}$. Thus ρ_g is a permutation.

Lastly, we will show that ρ is a homomorphism. Let $g_1, g_2 \in G$. Then $\rho_{g_1}\rho_{g_2}(x) = g_1g_2x = \rho_{g_1g_2}(x)$. It follows that $\rho(g_1g_2) = \rho_{g_1g_2} = \rho_{g_1}\rho_{g_2}$. Therefore ρ is a homomorphism. □

Definition 2.1.26. [8] The homomorphism ρ in Theorem 2.1.25 is called a *permutation representation* of G. If the kernel of the ρ is trivial then the action of G on X is called $faithful$.

Theorem 2.1.27. Burnside's Lemma *Let G act on X, where G is a group and X is a non-empty set. Then the number of orbits of G on X is*

$$\frac{1}{|G|}\sum_{g\in G}|X^g|,$$

where $|X^g|$ is the number of elements of X fixed by g.

Proof. Let $T = \{(g, x) \in G \times X : gx = x\}$ and $X = X_1 \cup X_2 \cup ... \cup X_k$ where the X_is are the distinct orbits of X and $x_i \in X_i$ for $1 \leq i \leq k$. Since $|X^g|$ is the number of elements of X fixed by g, we have $|T| = \sum_{g\in G}|X^g|$. On the other hand, since $|G_x|$ is the number of elements of G fixing x, then $|T| = \sum_{x\in X}|G_x|$. Therefore,

$$\sum_{g\in G}|X^g| = \sum_{x\in X_1}|G_x| + \sum_{x\in X_2}|G_x| + ... + \sum_{x\in X_k}|G_x|.$$

By the Orbit-Stabiliser Theorem (2.1.18), if two distinct elements of X are in same orbit, then the order of their stabilisers will be same. Hence, $\sum_{x\in X_i}|G_x| = |X_i||G_{x_i}|$. It follows that,

$$\sum_{g\in G}|X^g| = |X_1||G_{x_1}| + |X_2||G_{x_2}| + ... + |X_k||G_{x_k}|.$$

$$= \frac{|G|}{|G_{x_1}|}|G_{x_1}| + \frac{|G|}{|G_{x_2}|}|G_{x_2}| + ... + \frac{|G|}{|G_{x_k}|}|G_{x_k}|.$$

Thus $\sum_{g\in G}|X^g| = k|G|$, where k is the number of orbits of G on X. □

2.1.3 Sylow theorems

In this section, we will prove Sylow theorems. We first give some definitions and theorems that we use in the proofs of Sylow theorems. A group G will be finite.

Definition 2.1.28. Let p be a prime number and G be a group. A group G is called p-group if its order is a power of p.

Lemma 2.1.29. *Let G act on X, where G is a p-group and X is a non-empty set. Let X^G be a set of fixed points in the action as follows;*

$$X^G = \{x \in X : gx = x \ for \ all \ g \in G\}.$$

Then $|X^G| \equiv |X| \ mod \ p$.

Proof. Let X be a union $X_1 \cup X_2 \cup ... \cup X_k$, where X_i's are all distinct orbits of X for $1 \leq i \leq k$. Without loss of generality, we suppose that $|X_i| = 1$ for $1 \leq i \leq j$ and $|X_i| > 1$ for $j+1 \leq i \leq k$. Therefore,

$$|X^G| = X_1 \cup X_2 \cup ... \cup X_j,$$

and so $|X^G| = j$. Then,

$$|X| = |X^G| + \sum_{i=j+1}^{k} |X_i|. \tag{2.1}$$

Also by the Orbit-Stabiliser Theorem (2.1.18), we have $|X_i| = \frac{|G|}{|G_{x_i}|}$, where $x_i \in X_i$ for $1 \leq i \leq k$. It follows that since the order of G is a power of p, $|X_i|$ is also a power of p for $1 \leq i \leq k$. Therefore $|X_i| = p^0 = 1$ for $1 \leq i \leq j$ and $|\sum_{i=j+1}^{k} |X_i||$ is a multiple of p.

Then in *mod* p, (2.1) becomes $|X| \equiv j = |X^G|$. □

Theorem 2.1.30. Lagrange's Theorem *Let H be a subgroup of a group G. Then the order of H divides the order of G and the ratio is equal to the index of H in G, namely*

$$\frac{|G|}{|H|} = [G : H].$$

Proof. Let H be a subgroup of G. By Corollary 2.1.15.1, G can be partitioned into cosets of H. Then let $g_1H, g_2H, ..., g_nH$ be all distinct cosets of H in G. Thus $G = g_1H \cup g_2H \cup ... \cup g_rH$ and $|G| = |g_1H| + |g_2H| + ... + |g_nH|$. Since $|H| = |g_iH|$ for all $1 \leq i \leq n$ by Theorem 2.1.16, $|G| = n|H|$. Therefore $|H|$ divides $|G|$ and $n = [G : H]$. □

Lemma 2.1.31. [10, 1.8. Lemma] *Let p be a prime number; and let $r \geq 0$ and $m \geq 1$ be integers. Then*

$$\binom{p^r m}{p^r} \equiv m \ mod \ p.$$

Proof. Let n be a positive integer such that $(1+x)^n$ is polynomial. Then by binomial expansion,

$$(1+x)^n = x^n + \binom{n}{n-1}x^{n-1} + ... + \binom{n}{n-k} + ... + \binom{n}{1} + 1$$

where $1 \leq k \leq n-1$ and $\binom{n}{n-k}$'s are called *binomial coefficients.*

When $n = p$,

$$(1+x)^p = x^p + \binom{p}{p-1}x^{n-1} + ... + \binom{p}{p-k} + ... + \binom{p}{1} + 1$$

where $1 \leq k \leq p-1$.

We note that all $\binom{p}{p-k}$ in the above expansion are divisible by p since $k < p$ and p is prime. Hence we have $(1+x)^p \equiv 1 + x^p \ mod \ p$. This means that binomial

coefficients of corresponding powers of x are congruent $mod\ p$. If we take p power of each congruence sides then we have

$$((1+x)^p)^p \equiv (1+x^p)^p \equiv 1+(x^p)^p \equiv 1+x^{p^2}\ mod\ p.$$

If we keep continuing in this way, we have $(1+x)^{p^r} \equiv 1+x^{p^r}\ mod\ p$. It follows that

$$(1+x)^{p^r m} \equiv (1+x^{p^r})^m\ mod\ p. \tag{2.2}$$

Therefore we have $\binom{p^r m}{p^r} x^{p^r} \equiv \binom{m}{1} x^{p^r}\ mod\ p$ from out last congruence relation 2.1, and so

$$\binom{p^r m}{p^r} \equiv m = \binom{m}{1}\ mod\ p.$$

□

Definition 2.1.32. Let G be a group and p be a prime number.

(i) Let $|G|$ be $p^r m$ where $p \nmid m$ and $r \geq 0$. If there exists a subgroup P of order p^r then P is called a *Sylow p-subgroup* of G.

(ii) The set of all Sylow p-subgroups of G is denoted by $Syl_p(G)$.

(iii) The number of Sylow p-subgroups of G is denoted by n_p.

Now, we are ready to prove the existence theorem of Sylow.

Theorem 2.1.33. Sylow's Existence Theorem[10] *Let G be a group with order $|G| = p^r m$, where $p \nmid m$ and $r \geq 1$. Then there exists a Sylow p-subgroup in G.*

Proof. Let X be the set of all subsets with order p^r in G. Then G can act by right multiplication on X, and so X can be partitioned into orbits. This means that the order of X is a summation of the order of orbits. The order of X is simply $\binom{p^r m}{p^r}$. We note that $\binom{p^r m}{p^r} \equiv m\ mod\ p$ by Lemma 2.1.31. Hence $p \nmid |X|$ and there exists an orbit, say X_k, such that $p \nmid |X_k|$.

Let A be a subset in G such that $A \in X_k$. Also let G_A be the stabiliser of A in G. By the Orbit-Stabiliser Theorem 2.1.18, we have $|X_k| = \frac{|G|}{|G_A|}$. Also since $p \nmid |X_k|$ and $p^r \mid |G|$, p^r divides $|G_A|$. This means that $p^r \leq |G_A|$.

Let $a \in A$ and $h \in G_A$. Then $ah \in Ah = A$. This means that $aG_A \subseteq A$. Since $|G_A| = |aG_A|$, we have $|G_A| \leq |A| = p^r$. Hence the order of G_A is p^r. Therefore G_A is a Sylow p-subgroup of G. □

Hence we know that a Sylow p-subgroup exists in a group G. Next, we prove the remaining Sylow theorems.

Theorem 2.1.34. Sylow Theorems[9] *Let G be a group with order $|G| = p^r m$, where $p \nmid m$ and $r \geq 1$.*

(i) Any two Sylow p-subgroups of G are conjugate in G and any p-subgroup of G is contained in a Sylow p-subgroup.

(ii) The number of Sylow p-subgroups of G, n_p, is congruent to 1 mod p, namely $n_p \equiv 1$, and n_p divides $|G|$.

Proof. We have shown that there exists a Sylow p-subgroup P in G in Theorem 2.1.33. Then let X be the set of all conjugates of P, namely $X = \{gPg^{-1} := P^g : g \in G\}$. Thus P acts on X by conjugation. Since P is a p-group, $|X| \equiv |F_P(X)|$ *mod* p, where $F_P(X) = \{Q \in X : Q^g = Q \ for \ all \ g \in P\}$, by Lemma 2.1.29.

Obviously P is in $F_P(X)$ and so $F_P(X) \neq \emptyset$. Then let $Q \in F_P(X)$, and so $gQg^{-1} = Q$ for all $g \in P$. This means that $P \leq N_G(Q)$. Also since $Q \trianglelefteq N_G(Q)$, PQ is a group such that $P \leq PQ \leq N_G(Q)$. It follows that $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^k$ for some $k \leq r$. Since P and Q are both Sylow p-subgroups and $Q \leq PQ$, we have $PQ = P = Q$. Therefore $|F_P(X)| = 1$ and so $|X| = n_p \equiv 1$.

Let R be a p-subgroup of G. Then R acts on X by conjugation. By Lemma 2.1.29 and our previous work above, $|F_R(X)| \equiv |X| \equiv 1 \ mod \ p$. Therefore there is a $Q \in F_R(X)$ such that $gQg^{-1} = Q$ for all $g \in H$. Since $R \leq N_G(Q)$ and $Q \trianglelefteq N_G(Q)$, RQ is a group such that $Q \leq RQ \leq N_G(Q)$. This means that RQ is a p-subgroup of G containing Q, which is a Sylow p-subgroup. Hence we have $RQ = Q$. It follows that $R \leq RQ = Q$. Therefore any p-subgroup R is contained in a Sylow p-subgroup.

Let K be a Sylow p-subgroup of G. In our above argument, R can be K. Then $K \leq Q$ for some $Q \in X$. Since both K and Q are Sylow p-subgroups, they have same order. This means that $K = Q$. Therefore the set X contains all Sylow p-subgroups of G, and so any two Sylow p-subgroups are conjugate.

Finally, we have shown that the order of X is the number of conjugates of P. Thus $|X| = [G : N_G(P)]$ by Proposition 2.1.23. It follows that $m = [G : P] = [G : N_G(P)][N_G(P) : P]$. Hence $|X|$ divides m. □

Theorem 2.1.35. Cauchy's Theorem[10] *Let G be a group and its order $|G|$ be divisible by prime p. Then G has an element of order p.*

Proof. By Sylow's Existence Theorem (2.1.33), we know that there exists a Sylow p-subgroup of G, say P. Then $|P| = p^r$ where p^r is the highest power of p dividing the order of G. Let x be non-identity element of P. By Lagrange's Theorem (2.1.30), the order of x, say $|\langle x \rangle|$, divides $|P|$. Since x is not identity, $1 < |\langle x \rangle| = p^m$ for some $1 \leq m \leq r$. It follows that the order of x^m is p. Hence G has an element of order p. □

2.1.4 k-transitive actions

In this section, we will develop simplicity criterias for multiply transitive groups. The last two results of this section will help to show the simplicity of the Mathieu

groups M_{12}, M_{24} and M_{22}.

Definition 2.1.36. Let G act on X, where G is a group and X is a non-empty set. If there exists only one orbit of G then the action of G is called *transitive*. In other words; for any $x, y \in X$ there exists a $g \in G$ such that $x = gy$.

Definition 2.1.37. Let G act on X, where G is a group and X is a non-empty set. The action is called *k-transitive* if for any two ordered k-tuples $(x_1, ..., x_k), (y_1, ..., y_k)$ of distinct elements of X there exists a $g \in G$ such that $x_i = gy_i$ for $1 \leq i \leq k$, where $k \geq 1$. We may call our action in Definition 2.1.36 1-*transitive*. When $k \geq 2$, we may call our actions *multiply transitive* and our groups in the action *multiply transivite groups*.

Definition 2.1.38. If G acts transitively on a set X then the number of orbits of the stabiliser G_x on X is called *rank*.

The next theorem is fundamental for k-transitive actions.

Theorem 2.1.39. *Let G act transitively on X and $x \in X$. Then G acts k-transitively on X if and only if the stabiliser G_x acts $(k-1)$-transitively on $X \setminus \{x\}$, where $k \geq 2$.*

Proof. Suppose that G acts k-transitively on X. Then let $(x_1, ..., x_{k-1})$ and $(y_1, ..., y_{k-1})$ be ordered $(k-1)$-tuples of $X \setminus \{x\}$, where all x_i and y_i's are distinct entries of tuples. Also let $(x_1, ..., x_{k-1}, x)$ and $(y_1, ..., y_{k-1}, x)$ be k-tuples of X. It follows that there exists a $g \in G$ such that $x_i = gy_i$ for $1 \leq i \leq k-1$ and $x = gx$. Thus $g \in G_x$ and so G_x acts $(k-1)$-transively on $X \setminus \{x\}$.

Conversely, suppose that G_x acts $(k-1)$-transitively on $X \setminus \{x\}$. Let $(y_1, ..., y_k)$ be ordered k-tuple of X, where all y_i's are distinct entries of a tuple and also let $x_2, ..., x_k$ be distinct elements of $X \setminus \{x\}$. Since G acts transitively on X, there exists $g \in G$ such that $gy_k = x$ and $gy_i = z_i$ for $1 \leq i \leq k-1$. That is, $g(y_1, ..., y_{k-1}, y_k) = (z_1, ..., z_{k-1}, x)$. Since G_x acts $(k-1)$-transitively on $X \setminus \{x\}$, there exists $h \in G_x$

such that $hz_i = x_i$ for $1 \leq i \leq k-1$. Hence $h(z_1, ..., z_{k-1}, x) = (x_1, ..., x_{k-1}, x)$. This means that there exists $hg = f \in G$ such that $f(y_1, ..., y_k) = (x_1, ..., x)$. Therefore G acts k-transitively on X. □

Definition 2.1.40. Let G be a group and X be a non-empty set. Then let $H = \{x_1, ..., x_k\}$ be a subset of distinct elements of X. If G acts on X then the *pointwise stabiliser* of H in G is the set $\{g \in G : gx_i = x_i \; for \; 1 \leq i \leq k\}$ and denoted by $G_{x_1,...,x_k}$.

Definition 2.1.41. Let G act k-transitively on a non-empty set X. If only the identity element of G fixes k distinct elements of X then the action is called *sharply k-transitive*.

Now we will show the Orbit-Stabiliser relation of k-transitive and sharply k-transitive actions.

Theorem 2.1.42. *Let G act k-transitively on a non-empty set X. Then*

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

where $|X| = n$ and x_i's are all distinct elements of X.

Proof. Let G acts k-transitively on X and $x_1, ..., x_k$ be distinct elements of X. By Orbit-Stabiliser Theorem (2.1.18), we have $|G| = n|G_{x_1}|$. Since G acts k-transitively, G_{x_1} acts $(k-1)$-transively on $X \setminus \{x_1\}$. Then if we apply Orbit-Stabiliser Theorem on G_{x_1}, we have $|G_{x_1}| = (n-1)|G_{x_1,x_2}|$. In a similar manner, since G_{x_1,x_2} acts $(k-2)$-transitively on $X \setminus \{x_1, x_2\}$, we have $|G_{x_1,x_2}| = (n-2)|G_{x_1,x_2,x_3}|$. If $k \leq 3$, our process is already finished.

If we continue $(k-3)$ times more in this way for $k \geq 4$, then we have $|G_{x_1,...,x_{k-1}}| = (n-(k-1))|G_{x_1,...,x_k}|$.

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

Corollary 2.1.42.1. *If G acts sharply k-transitively on X, then*

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

Proof. Since G acts sharply, only the identity fixes $x_1, ..., x_k$. Thus $|G_{x_1,...,x_k}| = 1$. □

Theorem 2.1.43. *Let G act faithfully and k-transitively on X and $x \in X$. Then G acts sharply k-transitively on X if and only if the stabiliser G_x acts sharply $(k-1)$-transitively on $X \setminus \{x\}$, where $k \geq 2$.*

Proof. Suppose that G acts sharply k-transitively. Let $x \in X$. By Theorem 2.1.39, G_x acts $(k-1)$-transitively on $X \setminus \{x\}$. Let $(x_1, ..., x_{k-1})$ be ordered $(k-1)$-tuple of $X \setminus \{x\}$, where all x_i's are distinct. Since G acts sharply, the identity element of G is the only element fixing $(x_1, ..., x_{k-1}, x)$. This means that the identity element is also the only element of G_x fixing $(x_1, ..., x_{k-1})$. Therefore G_x acts sharply $(k-1)$-transitively.

Conversely, suppose that G_x acts sharply $(k-1)$-transitively on $X \setminus \{x\}$. Then by Theorem 2.1.39, G acts k-transitively on X. Let $(x_1, ..., x_k)$ be ordered k-tuple of X, where all x_i's are distinct and let $g \in G_{x_1,...,x_k}$. Then G_{x_i} acts sharply $(k-1)$-transitively on $X \setminus x_i$ for $1 \leq i \leq k$. For this reason, the identity element is the only element fixing $(x_1, ..., x_k)$. Hence g is the identity element, and so G acts sharply k-transitively on X. □

Definition 2.1.44. A sharply 1-transitive group action is called *regular*.

2.1.4.1 Primitive actions

Definition 2.1.45. Let G acts on X, where G is a group and X is a non-empty set. A *block* is a subset, say B, of X with special property: for all $g \in G$, either

$gB = B$ or $gB \cap B = \emptyset$. Then if B is empty set, X or one-point subset of X then we call B *trivial block*. If B is not previously mentioned trivial block then we call B *non-trivial block*.

Definition 2.1.46. Let G act transitively on X. If all blocks are trivial then G acts *primitively* on X. If there exists a non-trivial block then G acts *imprimitively* on X.

Theorem 2.1.47. *If G acts k-transitively on X, where $k \geq 2$, then the action is primitive.*

Proof. We suppose that there exists a non-trivial block in X, say B. Then let x_1, x_2, x_3 be distinct elements in X such that $x_1, x_2 \in B$ and $x_3 \notin B$. Since $k \geq 2$, there exists $g \in G$ such that $gx_1 = x_1$ and $gx_2 = x_3$. Thus $B \cap gB \neq \emptyset$ and so we get a contradiction. □

In the previous theorem, we show that if $k \geq 2$ then k-transitive actions are primitive. Now we will prove the fundamental theorem of primitive actions.

Theorem 2.1.48. *Let G act transitively on X. Then the action is primitive if and only if the stabiliser G_x is a maximal subgroup of G for all x X.*

Proof. We suppose that G_x is not a maximal subgroup. Thus there exists a subgroup H such that $G_x < H < G$. Let $Hx = \{gx : g \in H\}$ and suppose that $Hx \cap gHx \neq \emptyset$. Then there exist $h_1, h_2 \in H$ such that $h_1 x = gh_2 x$, and so $x = h_1^{-1} gh_2 x$. Thus we have $h_1^{-1} gh_2 \in G_x < H$. This implies that $g \in H$. Therefore $Hx = gHx$ and so Hx is a block.

Since $H > G_x$, Hx is non-empty. We suppose that $Hx = X$. Let us pick $g \in G$ such that $g \notin H$. Then there exists $h \in H$ such that $hx = y$ for all $y \in X$. That is, $gx = hx$ for some $h \in H$. It follows that $g^{-1}h \in G_x < H$. Thus $g \in H$ and so we

get a contradiction. Lastly, we suppose that Hx is a one-point subset of X. Thus $H \leq G_x$. Since $G_x < H$, we get a contradiction. Hence the action is not primitive.

Now, we suppose that G_x is a maximal subgroup and also there exists a non-trivial block, say B, in X. Let H be $\{g \in G : gB = B\}$. H is clearly a subgroup of G. Let $x \in B$. If $gx = x$ then $x \in B \cap gB$ and $g \in G_x$. Hence $gB = B$ and $G_x \leq H$. Since B is non-trivial, there exists $y \in B$ such that $x \neq y$. Also since the action is transitive, there exists $g \in G$ such that $gx = y$. This means that $y \in B \cap gB$ and so $gB = B$. Hence $g \in H$ but $g \notin G_x$. Thus $G_x < H$. Assume that $H = G$. Since G acts transitively, $X = B$. Then we get a contradiction. Hence we have $G_x < H < G$. Since G_x a maximal subgroup, we get a contradiction. □

2.1.4.2 Simplicity criteria

We first establish a relation between k-transitive action of a group G and normal subgroup H in G.

Definition 2.1.49. Let G be a group and H be a subgroup of G. If $gHg^{-1} = H$ for all $g \in G$ then H is called *normal subgroup* of G and the relation is denoted by $H \lhd G$.

Definition 2.1.50. Let G be a group such that $G \neq \{1\}$. G is called *simple* if G has only trivial normal subgroups, namely $\{1\}$ and G.

Definition 2.1.51. Let G act on X and $H \lhd G$. If H acts regularly on X then H is called *regular normal subgroup*.

Theorem 2.1.52. *Let G act on X and x, y be in X. Assume that H is subgroup of G. Then if $Hx \cap Hy \neq \emptyset$ we have $Hx = Hy$. If we assume that H is a normal subgroup then we call Hx block for any $x \in X$.*

Proof. We suppose that $Hx \cap Hy \neq \emptyset$. Then there exist $h_1, h_2 \in H$ such that $h_1x = h_2y$. Thus $x = h_1^{-1}h_2y$ and so $x \in Hy$. This implies that $Hx = Hy$.

Let $g \in G$. Now, we suppose that H is a normal subgroup of G and $gHx \cap Hy \neq \emptyset$. It follows that $gHx \cap Hx = Hgx \cap Hx$. Then there exist $h_1, h_2 \in H$ such that $h_1gx = h_2x$. Thus $gx = h_1^{-1}h_2x$ and so $gx \in Hx$. This implies that $gHx = Hy$; hence Hx is a block of G. □

Theorem 2.1.53. *Let G act faithfully and primitively on X. If H is non-trivial normal subgroup of G then H acts transitively on X.*

Proof. We know that for all $x \in X$, Hx is a block from Theorem 2.1.52. Then Hx must be one of the trivial blocks since G acts primitively. It follows that Hx can not be empty set or $\{x\}$ since H is non-trivial subgroup and G acts faithfully. Therefore $Hx = X$ for all $x \in X$ and so H acts transitively on X. □

Theorem 2.1.54. *Let G act faithfully and primitively on X and G_x be simple. Then we have either G is simple or every non-trivial normal subgroup H of G is a regular normal subgroup.*

Proof. If H is a non-trivial normal subgroup then H acts transitively on X by Theorem 2.1.53. It follows that $H \cap G_x \lhd G_x$ for all $x \in X$. Since G_x is simple, $H \cap G_x$ must be equal to 1 or G_x. If $H \cap G_x = 1$ then H acts regularly on X. Then if $H \cap G_x = G_x$ then $G_x \leq H$. By Theorem 2.1.48, G_x must be maximal subgroup of G. This means that $H = G$ since H acts transitively on X. □

Definition 2.1.55. Let G act on two non-empty sets X and Y. A function $f : X \longmapsto Y$ defined by $f(gx) = gf(x)$ for all $g \in G$ and $x \in X$ is called *G-map*. If f is a bijection then we call f *G-isomorphism* and say that two actions are *isomorphic*.

Theorem 2.1.56. *Let G act transitively on X and H be a regular normal subgroup of G. Let x be fixed in X and G_x act on $H^* := H \setminus \{1\}$ by conjugation. Then the actions of G_x on $X \setminus \{x\}$ and $H \setminus \{1\}$ are isomorphic.*

Proof. Let us define $f : H^* \longmapsto X \setminus \{x\}$ by $f(h) = hx$. Suppose that $f(h_1) = f(h_2)$ for some $h_1, h_2 \in H^*$. Then $h_1x = h_2x$ implies that $h_2^{-1}h_1 \in H_x$, and so f is one-to-one. Also since H acts regularly on X, $|X| = |H|$. Then $|H^*| = |X \setminus \{x\}|$ and f is onto. Therefore f is a bijection.

Now, we show that f is a G_x-map. Let $g \in G_x$ and $h \in H^*$. Then $f(gh) = f(ghg^{-1}) = ghg^{-1}x = ghx = gf(h)$. Therefore f is a G_x-map. □

Definition 2.1.57. Let p be a prime. An *elementary abelian group* is a group that is isomorphic to $\mathbb{Z}_p \times ... \times \mathbb{Z}_p$.

Now, we are ready to give simplicity criteria for k-transitive groups.

Theorem 2.1.58. [8] *Let G act k-transitively on X and H be a regular normal subgroup of G, where $2 \leq k$ and $|X| = n$. Then $k \leq 4$. Also,*

(i) If $2 \leq k \leq 4$ then H is an elementary p-group and $|X| = n = p^k$ for some p and k.

(ii) If $3 \leq k \leq 4$ then either $H \cong \mathbb{Z}_3$ and $n = 3$ or H is an elementary 2-group and $|X| = n = 2^k$ for some k.

(iii) If $k = 4$ then $H \cong \mathbf{V} = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $|X| = n = 2^2$.

Proof. Since G acts k-transitively on X, G_x acts $(k-1)$-transitively on $X \setminus \{x\}$ by Theorem 2.1.39. Then by Theorem 2.1.56, G_x acts $(k-1)$-transitively on $H \setminus \{1\} := H^*$ by conjugation.

(i) Since elements of H^* are conjugate in G, all elements in H^* have same order that is prime, say p. Hence $|H| = p^k$ for some k. Since H acts regularly on X, $|X| = n = p^k$. Also since the center of H is the H itself, H is abelian, and so H is an elementary abelian p-group.

(ii) Since $k \geq 3$, G_x acts primitively on H^* by Theorem 2.1.47. Let $h \in H^*$. Then $\{h, h^{-1}\}$ is a block since G_x acts by conjugation. It follows that $\{h, h^{-1}\}$ should be either H^* or $\{h\}$. If $\{h, h^{-1}\} = H^*$ then $H = \{1, h, h^{-1}\}$ and so $H \cong \mathbb{Z}_3$ and $|X| = 3$. If $\{h, h^{-1}\} = \{h\}$ then $h^2 = 1$ and so H is an elementary 2-group and $|X| = n = 2^k$ for some k.

(iii) We suppose that $k = 4$. Then $k - 1 = 3$ and $|X| \geq 4$ and by Theorem 2.1.56, $|X \setminus \{x\}| = |H^*|$. Thus $|H^*| \geq 3$. From part (ii), we have H is an elementary 2-group and since $|X| \geq 4$, H contains $\mathbf{V}$. Let $\mathbf{V} = \{1, h, k, hk\}$. Then G_{x_h} acts 2-transitively on $H^* \setminus \{h\}$. Hence this action also is primitive by Theorem 2.1.47. Then $\{k, hk\}$ is a block since G_{x_h} acts by conjugation. Therefore $\{k, hk\} = H^* \setminus \{h\}$ and so $H = \mathbf{V} = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $|X| = 4$. □

Theorem 2.1.59. [8] *Let G act faithfully and k-transitively on X, where $k \geq 2$, $|X| = n$ and G_x be simple for some $x \in X$.*

(i) If $k \geq 4$ then G is simple.

(ii) If $k \geq 3$ and $|X| \neq 2^k$ for some k then either $G \cong S_3$ or G is simple.

(iii) If $k \geq 2$ and $|X| \neq p^k$ for any k and prime p then G is simple.

Proof. Since G acts faithfully and primitively on X and G_x is simple, we have either G is simple or G has regular normal subgroup H. We suppose that G has regular normal subgroup H. By Theorem 2.1.58, $k \leq 4$ and if $k = 4$ we have $H \cong \mathbf{V}$ and $|X| = 4$. Also let ρ be a permutation representation of the action of G on X. Thus $\rho(G) \leq S_4$. It follows that S_4 has only 4-transitive subgroup that is itself and the stabiliser of any point in S_4 is S_3 that is not simple. Therefore we get a contradiction. Hence G is simple.

If we have $k \geq 3$ and $|X| \neq 2^k$ for some k then we get $H \cong \mathbb{Z}_3$ and $n = 3$ by

Theorem 2.1.58. This means that $\rho(G) \leq S_3$. Since S_3 has only 3-transitive subgroup that is itself and the stabiliser of any point in S_3 is S_2 that is simple, we have either $G \cong S_3$ or G is simple.

If we have $k \geq 2$ then we have $|X| = n = p^k$ for some p and k by Theorem 2.1.58. Therefore we get a contradiction and so G is simple. □

2.2 Affine and projective planes

In this section, we mainly follow G. Eric Moorhouse's book [12] and Bart De Bruyn's book [13]. We will explain basic properties of finite affine and projective spaces. In chapter 4, we will see that these finite geometries have a connection with certain Steiner systems.

2.2.1 Introduction

Definition 2.2.1. An *incidence structure* contains two certain objects together with a binary relation that shows an incidence relation between these objects.

Throughout our discussion, we will consider certain objects as points and lines.

Definition 2.2.2. A *point-line incidence structure* is an $S = (\mathcal{P}, \mathcal{L}, I)$ where $\mathcal{P}$ is a set of points, $\mathcal{L}$ is a set of lines and I is the incidence relation. In other words, I is a subset of $\mathcal{P} \times \mathcal{L}$, which means that it is a binary relation showing which pairs of point-line are incident.

We will show an example of the classical point-line incidence structure.

Example 2.2.3. Let $\mathcal{P} = \mathbb{R}^2$, where $\mathbb{R}$ is the set of real numbers and let $\mathcal{L}$ be the set of straight lines incident with $(x, y) \in \mathbb{R}^2$. Then I is a set containment. Thus S becomes the Euclidean Plane.

Definition 2.2.4. If a point-line incidence structure satisfies following properties:

(i) There exists at most one line through any two distinct points.

(ii) Every line contains at least two points.

then call it *partial linear space*.

Definition 2.2.5. If a point-line incidence structure satisfies following properties:

(i) There exists exactly one line through any two distinct points.

(ii) Every line contains at least two points.

then call it *linear space*.

Now, we are ready to show some basic properties of our special examples of linear spaces: Affine and projective planes.

2.2.2 Affine planes

Definition 2.2.6. An $affine\ plane$ is a linear space satisfying following properties:

(i) For any line ℓ and any point x not on ℓ there exists exactly one line through x that does not meet ℓ.

(ii) There exists four points, no three of which are collinear.

Definition 2.2.7. Let ℓ and m be two lines in an affine plane. Then ℓ is *parallel* to m, denoted by $\ell \parallel m$, if either $\ell = m$ or ℓ and m have no common point.

Lemma 2.2.8. *Parallelism is an equivalence relation.*

Proof. Let ℓ, m, h be distinct lines. Firstly, $\ell \parallel \ell$, and so our relation is reflexive. Also if we have $\ell \parallel m$ then we have $m \parallel \ell$ too. Thus our relation is symmetric. Lastly, suppose that $\ell \parallel m$ and $m \parallel n$. We assume that ℓ and n are not parallel. Then they have a common point, say x. However m is parallel to both ℓ and n; and since $x \notin m$ there exists a unique line through x parallel to m. However there exist two lines that are incident to x. Therefore we get a contradiction. Then $\ell \parallel n$, and so our relation is transitive. Thus $\parallel$ is an equivalence relation. □

Theorem 2.2.9. *Let S be an affine plane. Any two lines in S contain the same number of points.*

Proof. Let ℓ_1 and ℓ_2 be two distinct lines. Then there exists a point $x \in \ell_1$ such that $x \notin \ell_2$. Similarly, there exists a point $y \in \ell_2$ such that $y \notin \ell_1$. Let ℓ_3 be a line that is incident to x and y. Also let z_1 be any point in ℓ_1. Hence there exists a line ℓ_4 that contains z_1 is parallel to ℓ_3. It follows that ℓ_4 is not parallel to ℓ_3, and so ℓ_4 contains a common point with ℓ_3, say $z_1^{'}$. We suppose that ℓ_1 contains n points for $n \geq 2$. Then we can repeat same procedure for the remaining $n-1$ points of ℓ_1. Therefore we have a bijection between ℓ_1 and ℓ_2. Hence ℓ_2 contains n points. □

Definition 2.2.10. The *order* of an affine plane is the number of points on the line of the plane.

If an affine plane is of order n then each line in an affine plane contains n points.

Theorem 2.2.11. *Let S be an affine plane of order $n \geq 2$. Then the following properties hold:*

(*i*) *Every point of S is incident with exactly $n+1$ lines.*

(*ii*) *Every parallel class of S is comprised of n lines.*

(*iii*) *There exists $n+1$ parallel classes in S.*

(*iv*) *There exists n^2 points in S.*

(*v*) *There exists n^2+n lines in S.*

Proof. (*i*) Let x and y be two distinct points of S. We know that for any line ℓ_1 through x there exists a unique line ℓ_2 through y that is parallel to ℓ_1. This means that there exists bijection between lines containing x and lines containing y. By Theorem 2.2.9, each line has n points such that $n+1$ is the number of lines through any point.

Let x, y and z be three non-collinear points. In addition to a line through x, y and a line through x, z, there exists a unique line through x parallel to the line through y, z. This means that we have at least three lines through x. Hence $n+1 \geq 3$.

(*ii*) Let $\mathcal{K}$ be a parallel class of S. Then let $\ell_1 \in \mathcal{K}$. We suppose that there is a point x in ℓ_1. Also let $x \in \ell_2$ such that $\ell_1 \neq \ell_2$. ℓ_2 contains $n-1$ points other than x. It follows that there exists a unique line that is parallel to ℓ_1 through for each $n-1$ points on ℓ_2. This means that $|\mathcal{K}| \geq n$. Also since there are n points on ℓ_2 and $\ell_2 \notin \mathcal{K}$, each line in $\mathcal{K}$ is incident with a point of ℓ_2. So $|\mathcal{K}| \leq n$. Therefore we have $|\mathcal{K}| = n$

(*iii*) Let x be a point. For every parallel class $\mathcal{K}$, there exists a unique line through x which is in $\mathcal{K}$. Also there exists $n+1$ lines that are incident with x. Hence there are $n+1$ different parallel classes.

(iv) Since parallelism is an equivalence relation, a parallel class partition the points of S. In each parallel class, there exist n lines and each line contains n points. Hence there are n^2 points in S.

(v) There are $n+1$ parallel classes and each containing n lines. Hence there exists $n(n+1)$ lines in S. □

2.2.3 Projective planes

Definition 2.2.12. A *projective plane* is a linear space satisfying following properties:

(i) Any two distinct lines have a unique common point.

(ii) There exists four points, no three of which are collinear.

Theorem 2.2.13. *If we remove a line from a projective plane then we will have an affine plane.*

Proof. We suppose that ℓ_1 is a line that is removed from the projective plane. Since we have a linear space, we only need to check properties of an affine plane. Let x be a point such that $x \notin \ell_1$ and ℓ_2 be a line such that $\ell_2 \neq \ell_1$ and $x \notin \ell_2$. Let $y = \ell_1 \cap \ell_2$. Then every line is incident with x intersects ℓ_2 in a point outside ℓ, apart form the line through x and y, which is the unique line through x parallel to ℓ_2.

Let x, y, z, w be four points in the projective plane such that no three of which are collinear. If ℓ_1 contains at most one of the x, y, z or w then the last property of an affine plane is satisfied by remaining three points. Without loss of generality, let $z, w \in \ell_1$. Let p be the common point of the line through x, z and the line through

y, w. Then we have $p \notin \ell_1$ and p not in the line through x, y. Therefore p, x, y satisfy the last property of an affine plane. Hence we have an affine plane. □

We will use Theorem 2.2.13 to prove basic properties of a projective plane in the next theorem.

Theorem 2.2.14. *Let S be a projective plane of order $n \geq 2$. Then the following properties hold:*

(*i*) *Every line of S contains exactly $n + 1$ points.*

(*ii*) *Every point of S is incident with exactly $n + 1$ lines.*

(*iii*) *There exists $n^2 + n + 1$ points in S.*

(*iv*) *There exists $n^2 + n + 1$ lines in S.*

Proof. By previous theorem, if we remove a line ℓ from the projective plane we get an affine plane. Let n be the order of the affine plane. Each affine line contains n points. Thus adding the removed point leads to $n + 1$ points on each line in the projective plane. There exist $n + 1$ lines that is through each point in the affine plane. If we have a removed point then there exists n affine lines through it. Then there are n^2 affine points and $n + 1$ points of the removed line. Also there are $n^2 + n$ affine lines and one removed line. □

Chapter 3

Steiner Systems

In this chapter, we will introduce Steiner systems and its some properties that we will use throughout the thesis. We mainly follow John D. Dixon and Brian Mortimer's book [16] *Permutation groups*.

3.1 Introduction

Definition 3.1.1. [17] Let t, k, v be integers such that $1 < t < k < v$. A *Steiner system* $S(t, k, v)$ is a set V of v points together with a family $\mathcal{B}$ of subset of k points, blocks, of V with the property that every subset of t points of V is contained in exactly one block.

Example 3.1.2. [18] The Fano Plane in Figure 3.1.1 is an example of the Steiner system of type $S(2, 3, 7)$ that is unique up to isomorphism. In the plane, there are 7 points that form a set V. Then a family $\mathcal{B}$ of subsets of 3 points is seen as 7 lines with the property that any two points of V lie in a unique line. Also we note that proving

strategy of the uniqueness of $S(2,3,7)$ is similar to the proof of the uniqueness of $S(2,3,9)$ in Theorem 5.1.1.

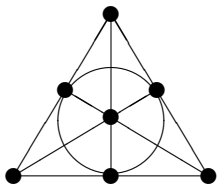

Figure 3.1.1 [18]: The Fano Plane

Now, we will count the number of blocks, namely $|\mathcal{B}|$. The number of subset of t points of V is $\binom{v}{t}$. Likewise, the number of subset of t points in each block is $\binom{k}{t}$. Since every subset of t points is contained in a unique block then $|\mathcal{B}|$ is equal to

$$\frac{\binom{v}{t}}{\binom{k}{t}}. \tag{3.1}$$

In a similar manner, we will count the number of blocks containing any given point, say α. Since α is fixed in blocks we consider set of points as $V \setminus \{\alpha\}$ and its order of blocks as $k-1$ in our further calculation. The number of subset of $t-1$ points of $V \setminus \{\alpha\}$ is $\binom{v-1}{t-1}$. Similarly, the number of subset of $t-1$ points containing α in each block containing α is $\binom{k-1}{t-1}$. Hence the number of blocks containing α is $\frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$.

This result can be extended to t points if we proceed in a same way. Therefore the number of blocks containing i points where $1 \leq i \leq t$ is equal to

$$\frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}. \tag{3.2}$$

Our observation and its generalization above lead to Theorem 3.2.1 in the following section that will play key role to the construction of Mathieu groups by Steiner systems.

3.2 Some properties

Theorem 3.2.1. *If there exists an $S(t,k,v)$ then there exists an $S(t-1,k-1,v-1)$ where $2 < t < k < v$.*

Proof. We suppose that an $S(t,k,v)$ exists. Then let β be any point in V. Our claim is that we can form a Steiner system on a set $V \setminus \{\beta\}$ of $v-1$ points.

Firstly; in $S(t,k,v)$ we exclude blocks not containing β. Hence we have gotten only blocks containing β. In these blocks, every subset of t points is contained in exactly one block. If we remove β from blocks containing β we have a sets of $k-1$ points and every subset of $t-1$ points is in a unique set of $k-1$ points. Therefore there exists an $S(t-1,k-1,v-1)$. □

We can generalize Theorem 3.2.1 as follows.

Corollary 3.2.1.1. *If there exists an $S(t,k,v)$ then there exists an $S(t-i,k-i,v-i)$ where $1 \leq i \leq t-2$.*

Proof. We suppose that an $S(t,k,v)$ exists. Then by Theorem 4.2.1., $S(t-1,k-1,v-1)$ exists. Hence $S(t-2,k-2,v-2)$ exists too. If we repeat this process $t-4$ times more we will get $S(2,k-t+2,v-t+2)$ that exists. □

Proposition 3.2.2. *If there exists $S(2,3,7)$ then there exists $S(3,4,8)$.*

Proof. We have already introduced the Fano Plane, $S(2,3,7)$, in Example 3.1.2. We assume that we already have an $S(3,4,8)$. Also by Corollary 3.2.1.1, if $S(3,4,8)$ exists then $S(2,3,7)$ exists too. As a result if we remove one point, say α, from $S(3,4,8)$ we will have $S(2,3,7)$. For this reason, a block in $S(3,4,8)$ containing α is

of the form $\Omega \cup \{\alpha\}$ where Ω denotes a block; that is, a line in $S(2,3,7)$. Since there are 7 such Ω, we have 7 such form of $\Omega \cup \{\alpha\}$.

We note that $\Omega \cup \{\alpha\}$ has three collinear points and α. Also the number of blocks in $S(3,4,8)$ is $\frac{\binom{8}{3}}{\binom{4}{3}} = 14$. We have already known seven blocks which are of the form $\Omega \cup \{\alpha\}$. Then there are remaining seven blocks that do not contain α or any three collinear points. That is, these blocks have 4 points from $S(2,3,7)$ and these points of no three are collinear.

In $S(2,3,7)$, there are $\binom{7}{4} = 35$ sets of four points in total. Now, we want to exclude sets which have three collinear points. Recall that there are seven lines. Hence, we pick a one line in $\binom{7}{1}$ different ways. Also, we choose a one further point out of four points those are not in the line that we have picked. Hence there are $\binom{7}{1}\binom{4}{1} = 28$ sets of four points containing three collinear points. Therefore there are 7 blocks that do not have three collinear points, and so we have found the remaining blocks for $S(3,4,8)$. Then $S(3,4,8)$ is a one-point extension of $S(2,3,7)$. □

Remark 3.2.3. A One-point extension of a Steiner system does not always exist. For example, there is no one-point extension of $S(3,4,8)$. If $S(4,5,9)$ exists then the number of blocks of $S(4,5,9)$ is $\frac{\binom{9}{4}}{\binom{5}{4}}$ but this is not an integer. Hence there is no such Steiner system of that type.

Definition 3.2.4. [17] Let $S(t,k,v)$ be a Steiner system, where V is a set of points and $\mathcal{B}$ is a family of blocks B. Let i and j be integers such that $0 \leq i,j \leq k$, and let N and M be disjoint subsets of B of sizes i and j, respectively. The number of blocks containing all elements of N but no elements of M is called the i,j-*intersection number* $\lambda_{i,j}$. The array $(\lambda_{i,j} : 0 \leq i+j \leq k)$ is the *intersection triangle* of a Steiner system.

We can immediately compute $\lambda_{i,0}$ as below by the formula (3.2).

$$\lambda_{i,0} = \begin{cases} \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} & \text{when} \quad 0 \leq i \leq t \\ 1 & \text{when} \quad t < i \leq k \ , \end{cases}$$

and we can easily observe that $\lambda_{i-1,1} = \lambda_{i-1,0} - \lambda_{i,0}$ for $i \geq 1$. Then $\lambda_{i-2,2} = \lambda_{i-2,1} - \lambda_{i-1,1}$ for $i \geq 2$. When we continue in this way, we get $\lambda_{i-j,j} = \lambda_{i-j,j-1} - \lambda_{i-j+1,j-1}$ for $1 \leq j \leq i$. Then we can rewrite this equation in a more general way, namely $\lambda_{i,j} = \lambda_{i,j-1} - \lambda_{i+1,j-1}$ for $j \geq 1$, by interchanging $i - j$ with i in the latter equation.

Example 3.2.5. We will give an example of the intersection triangle of a Steiner system $S = S(3, 4, 8)$ for Definition 3.2.4. The number of blocks in $S(3, 4, 8)$, namely $\lambda_{0,0}$, is $\frac{\binom{8}{3}}{\binom{4}{3}} = 14$. Let N and M be disjoint subsets of block B. Suppose that $|N| = |\{x\}| = 1$ and $|M| = 0$. Then the number of blocks containing x, $\lambda_{1,0}$, is $\frac{\binom{7}{2}}{\binom{3}{2}} = 7$. Likewise, suppose that $|N| = 0$ and $|M| = |\{x\}| = 1$. Hence the number of blocks containing x, $\lambda_{0,1}$, is $\frac{\binom{7}{2}}{\binom{3}{2}} = 7$.

Now, we look at the case where $|N| = |\{x, y\}| = 2$ and $|M| = 0$. Then the number of blocks containing x and y, $\lambda_{2,0}$, is $\frac{\binom{6}{1}}{\binom{2}{1}} = 3$. Likewise if $|N| = 0$ and $|M| = |\{x, y\}| = 2$ then the number of blocks containing x and y, $\lambda_{0,2}$, is $\frac{\binom{6}{1}}{\binom{2}{1}} = 3$.

Furthermore if $|N| = |\{x, y, z\}| = 3$ and $|M| = 0$ then the number of blocks, $\lambda_{3,0}$, is $\frac{\binom{5}{0}}{\binom{1}{0}} = 1$. Similarly if $|N| = 0$ and $|M| = |\{x, y, z\}| = 3$ then the number of blocks, $\lambda_{0,3}$, is $\frac{\binom{5}{0}}{\binom{1}{0}} = 1$.

Then we will examine the case that both N and M are non-empty. Suppose that $|N| = |\{x\}| = 1$ and $|M| = |\{y\}| = 1$. This means that we are looking for blocks containing x but not y. The number of blocks containing x and y, $\lambda_{2,0}$, is 3. Also the number of blocks containing x, $\lambda_{1,0}$, is 7. Since blocks containing x and y are included in blocks containing x, the number of blocks containing x but not y, $\lambda_{1,1}$, is

$7 - 3 = 4$, namely $\lambda_{1,1} = \lambda_{1,0} - \lambda_{2,0}$. In a similar reasoning we have $\lambda_{2,1} = \lambda_{2,0} - \lambda_{3,0}$ and $\lambda_{1,2} = \lambda_{1,1} - \lambda_{2,1}$.

At last, the intersection triangle of $S(3, 4, 8)$ is in as below.

$$14 = \lambda_{0,0}$$

$$7 = \lambda_{1,0} \qquad 7 = \lambda_{0,1}$$

$$3 = \lambda_{2,0} \qquad 4 = \lambda_{1,1} \qquad 3 = \lambda_{0,2}$$

$$1 = \lambda_{3,0} \qquad 2 = \lambda_{2,1} \qquad 2 = \lambda_{1,2} \qquad 1 = \lambda_{0,3}$$

Theorem 3.2.6. [16, Theorem 6.2A.] *Let $S(t, k, v)$ be a Steiner system with b blocks such that each point lies in exactly r blocks. Then*

(i) $bk = vr$,

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

Proof. Let V be a set of v points in $S(t, k, v)$ and let α be in V. Then we form a pair (α, B) such that α is in the block B. To prove our first assertion, we will count the number of pairs (α, B) in two ways.

We note that there are b blocks and in each blocks there are k points. Hence there are k options for choosing α and b options for choosing blocks. Therefore the number of pairs is equal to bk. Secondly, we have v options for choosing α from the set V and r options for choosing blocks containing α. Therefore the number of pairs is equal to vr. Hence $bk = vr$.

Now, we will prove the Fisher's inequality. We will define $S(t, k, v)$ by using incidence matrix $v \times b$, say M. Let α_i be points in V and B_j be blocks such that

$1 \leq i \leq v$ and $1 \leq j \leq b$. Hence we identify (i,j)-entries of M with α_1 and B_j such that (i,j)-entry will be 1 if $\alpha_i \in B_j$ and (i,j)-entry will be zero if otherwise.

Let M^T be *transpose* of M. Then M^T is a $b \times v$ matrix and MM^T is a $v \times v$ matrix. We note that (i,j)-entry of MM^T is the dot product of ith row of M with jth row of M. This means that (i,j)-entry gives us the number of blocks containing both α_i and α_j, say r_2. If $i = j$ then (i,j)-entry will be r that is the number of blocks containing α_i. By the formula (3.2),

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

and

$$r_2 = \frac{\binom{v-2}{t-2}}{\binom{k-2}{t-2}} = \frac{(v-2)(v-3)...(v-t+1)}{(k-2)(k-3)...(k-t+1)}.$$

Then we get $r_2\frac{(v-1)}{(k-1)} = r$. It follows that $r_2(v-1) = r(k-1)$. Since $1 < t < k < v$, $r > r_2$.

$$MM^T = \begin{bmatrix} r & r_2 & r_2 & ... & r_2 \\ r_2 & r & r_2 & ... & r_2 \\ r_2 & r_2 & r & ... & r_2 \\ ... & ... & ... & ... & ... \\ r_2 & r_2 & r_2 & ... & r \end{bmatrix}$$

MM^T is illustrated as above. Now we apply elementary row and column operations. Firstly; for this purpose, we add -1 multiple of first row to other rows. After that, we add second column to first column. Then we proceed as adding remaining $v-2$ columns to first column. Hence we have a matrix of the form:

$$U = \begin{bmatrix} r + r_2(v-1) & r_2 & r_2 & ... & r_2 \\ 0 & r - r_2 & 0 & ... & 0 \\ 0 & 0 & r - r_2 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & ... & r - r_2 \end{bmatrix}$$

Hence we have an upper-triangle matrix, and so $det(U)$ is the multiplication of diagonal entries. Our operations to MM^T do not affect the determinant, namely $det(MM^T) = det(U)$. Therefore $det(MM^T) = (r + r_2(v+1))(r - r_2)^{v-1}$. Since $r > r_2$, $det(MM^T) \neq 0$. This means that MM^T is $v \times v$ invertible matrix, and so it has rank v. For this reason the $v \times b$ matrix M also has rank v, thus $v \leq b$.

Since $v \leq b$ and $bk = vr$, we have $k \leq r$. Therefore we have proved Fisher's inequality. □

To sum up, we can find b and r from t, k, v. For this reason we do not need to show b and r in our notation $S(t, k, v)$. Moreover from Theorem 3.2.6, we note that t, k and v must be an integer. Also the number of blocks containing i points, calculated by the formula (3.2), that we have shown before must be an integer. Therefore we have shown necessary conditions on the parameters of a Steiner system.

Next we will show the connection between finite geometries and Steiner systems since in chapter 4 and 5, we will use the properties of affine and projective planes.

Theorem 3.2.7. [13] *$S(2, n+1, n^2+n+1)$ is a projective plane of order n, where $n \geq 2$.*

Proof. We suppose that $\mathcal{S}$ is a projective plane of order n. Then $\mathcal{S}$ contains n^2+n+1 points and every line is incident to exactly $n+1$ points by Theorem 2.2.14. Also

every two distinct points determine the unique line. Hence $\mathcal{S}$ is $S(2, n+1, n^2+n+1)$ Steiner system by Definition 3.1.1.

For the converse, we suppose that $\mathcal{S}$ is an $S(2, n+1, n^2+n+1)$. Since there exist exactly one line through any two distinct points and every line is through at least two points, $\mathcal{S}$ is a linear space by Definition 2.2.5. Also since $\mathcal{S}$ contains n^2+n+1 points and every line is incident with exactly $n+1$ points, there exist $n+1$ lines through each point. Let ℓ_1 and ℓ_2 be two distinct lines ℓ_1 and ℓ_2 such that $x \in \ell_2 \setminus \ell_1$. Since ℓ_1 contains $n+1$ points, there exist $n+1$ lines through x meeting ℓ_1. Since these are the complete set of lines through x, the lines ℓ_1 and ℓ_2 must have an intersection. Hence $\mathcal{S}$ is a projective plane of order n by Definition 2.2.12. □

Theorem 3.2.8. [13] *$S(2, n, n^2)$ is an affine plane of order n, where $n \geq 2$.*

Proof. We suppose that $\mathcal{S}$ is an affine plane of order n. Then $\mathcal{S}$ contains exactly n^2 points and every line is incident with exactly n points by Theorem 2.2.11. Also every two distinct points determine the unique line. Hence $\mathcal{S}$ is $S(2, n, n^2)$ Steiner system by Definition 3.1.1.

For the converse, we suppose that $\mathcal{S}$ is an $S(2, n, n^2)$. Since there exist exactly one line through any two distinct points and every line is through at least two points, $\mathcal{S}$ is a linear space by Definition 2.2.5. Also since $\mathcal{S}$ contains n^2 points and every line is incident with n points, there exist $n+1$ lines though each point. Also we have $n+1 \geq 2$. Then there are three non-collinear points. It follows that there are exactly n lines through x contained in ℓ since ℓ contains n points. Hence there is a unique line m through x such that $m \neq \ell$. Hence $\mathcal{S}$ is an affine plane by Definition 2.2.6. □

3.3 Automorphisms of Steiner systems

Let S be a Steiner system with ordered pair $(V, \mathcal{B})$, where V is a set of points and $\mathcal{B}$ is a family of subsets of V. We denote S by $S(V, \mathcal{B})$.

Definition 3.3.1. [8] Let $S(V, \mathcal{B})$ be a Steiner system. An *automorphism* of $S(V, \mathcal{B})$ is a bijection f: $V \longmapsto V$ such that $B \in \mathcal{B}$ implies $f(B) \in \mathcal{B}$. That is to say, f permutes the blocks of S by permuting the points of S.

Theorem 3.3.2. [8] *The set of all automorphisms of a Steiner system $S(V, \mathcal{B})$ is a group.*

Proof. Let G be a set of all automorphisms of $S(V, \mathcal{B})$. Let e be an identity function such that $e(B) = B$ for any $B \in \mathcal{B}$. Thus $e \in G$, and so G is non-empty. Let f and h be in G. Now, we want to show that h^{-1} is an automorphism. Since all automorphism in G are permutations of V, G is a subset of S_V, symmetric group on V. Also since S_V is finite group, $h^{-1} = h^n$ for some $n > 0$. Hence h^n is an automorphism because composition of automorphisms is an automorphism too. Thus h^{-1} is an automorphism, and so h^{-1} is in G. Therefore fh^{-1} is also in G and hence G is a group. □

Remark 3.3.3. The group of automorphisms of $S(V, \mathcal{B})$ is denoted by $Aut(S(V, \mathcal{B}))$ or if $S(V, \mathcal{B}) = S(t, k, v)$ then its group of automorphisms may be denoted by $Aut(S(t, k, v))$.

Proposition 3.3.4. [16] *$Aut(S(V, \mathcal{B}))$ acts on both points of V and the blocks B.*

Proof. Let $\theta : Aut(S(V, \mathcal{B})) \times V \longmapsto V$ by $\theta(fv) = f(v)$ for all $f \in Aut(S(V, \mathcal{B}))$ and $v \in V$. We check two properties of a group action. Let $f_1, f_2 \in Aut(S(V, \mathcal{B}))$ and $v \in V$. Firstly, $ev = e(v) = v$, where e is the identity function. Secondly,

$f_1(f_2v) = f_1(f_2(v))$. Then $f_2(v) = v^{'}$ for some $v^{'} \in V$. It follows that $f_1(f_2v) = f_1(v^{'}) = (f_1f_2)(v)$. Hence this action satisfies group action criteria.

In a same manner, let $\eta : Aut(S(V,\mathcal{B})) \times \mathcal{B} \longmapsto \mathcal{B}$ by $\eta(fB) = f(B)$ for all $f \in Aut(S(V,\mathcal{B}))$ and $B \in \mathcal{B}$. We check two properties of a group action. Let $f_1, f_2 \in Aut(S(V,\mathcal{B}))$ and $B \in \mathcal{B}$. Firstly, $eB = e(B) = B$, where e is the identity function. Secondly, $f_1(f_2B) = f_1(f_2(B))$. Then $f_2(B) = B^{'}$ for some $B^{'} \in B$. It follows that $f_1(f_2B) = f_1(B^{'}) = (f_1f_2)(B)$. Hence this action satisfies group action criteria. □

Therefore we have shown that $Aut(S(V,\mathcal{B}))$ acts on both points of V and the blocks B. The next theorem we will deal with the connection of these actions.

Theorem 3.3.5. [16, Theorem 6.2B.] *Let $S(V,\mathcal{B})$ be a Steiner system and G be a group of automorphisms of $S(V,\mathcal{B})$, namely $Aut(S(V,\mathcal{B}))$. Then,*

(i) The number of orbits of an action of G on $\mathcal{B}$ is at least as great as the number of orbits of an action of G on V.

(ii) Let G act transitively on both $\mathcal{B}$ and V. Then the rank of G acting on $\mathcal{B}$ is at least as great as the rank of G acting on V.

Proof. (i) Let $V_1, V_2, ..., V_s$ be the orbits of G on V and $\mathcal{B}_1, \mathcal{B}_2, ..., \mathcal{B}_f$ be the orbits of G on $\mathcal{B}$. Also let us define $n_i := |V_i|$. Our aim is to show that $s \leq f$.

Now, let c_{ik} be the number of points in V_i that lie in any given block in $\mathcal{B}_k$ and d_{kj} be the number of blocks in $\mathcal{B}_k$ that contain a given point of V_j, where $1 \leq i, j \leq s$ and $1 \leq k \leq f$.

We fix i and j then define sets T_1, T_2 as

$$T_1 := \{(\alpha, B) \in V_i \times \mathcal{B}_k : \alpha \in B\},$$

$$T_2 := \{(B, \beta) \in \mathcal{B}_k \times V_j : \beta \in B\}.$$

Then the order of the sets as follows,

$$|T_1| = \sum_{k=1}^{f} c_{ik} \text{ and } |T_2| = \sum_{k=1}^{f} d_{kj} n_j.$$

Due to the definitions of c_{ik} and d_{kj}, we can combine the sets T_1 and T_2 to define a new set T. Then,

$$T := \{(\alpha, B, \beta) \in V_i \times \mathcal{B}_k \times V_j : \alpha, \beta \in B\}.$$

Therefore the order of the set T as follows,

$$|T| = \sum_{k=1}^{f} c_{ik} d_{kj} n_j.$$

Moreover, we try to compute $|T|$ in a different way. Firstly, let us pick α in V_i and β in V_j. By the formula 3.2 in the chapter 3, the number of blocks containing α and β is equal to $\frac{\binom{v-2}{t-2}}{\binom{k-2}{t-2}} := \lambda_2$ and the number of blocks containing one of the α and β is equal to $\frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}} := \lambda_1$ under the assumption that $S(V, \mathcal{B}) = S(t, k, v)$. Then we pick a block containing α and β.

More precisely, we firstly suppose that $i \neq j$. Then we pick α from V_i out of n_i options. Similarly, we pick β from V_j out of n_j options. Also the number of blocks containing α and β is λ_2. Therefore, the order of T is equal to $n_i n_j \lambda_2$.

Now, we suppose that $i = j$. We pick α from V_i out of n_i options. Similarly, we pick β from V_i out of $n_i - 1$ options. Also the number of blocks containing α and β is λ_2. Since α and β are in the same orbit, there is also one more case, that is

$\alpha = \beta$. In this case, we only pick one point, namely α. Then the number of blocks containing α is λ_1. Therefore the order of T is equal to $n_i(n_i-1)\lambda_2 + n_i\lambda_1$.

In summary,

$$|T| = \sum_{k=1}^{f} c_{ik}d_{kj}n_j = \begin{cases} n_i(n_i-1)\lambda_2 + n_i\lambda_1 \text{ if } i = j \\ n_i n_j \lambda_2 \qquad\qquad\qquad \text{if } i \neq j. \end{cases}$$

After dividing both sides by n_j,

$$\sum_{k=1}^{f} c_{ik}d_{kj} = \begin{cases} (n_i-1)\lambda_2 + \lambda_1 \text{ if } i = j \\ n_i\lambda_2 \qquad\qquad\qquad \text{if } i \neq j. \end{cases}$$

The term $\sum_{k=1}^{f} c_{ik}d_{kj}$ can be seen as the (i,j)th entry of the matrix which is the matrix multiplication of C and D, where C is an $s \times f$ matrix with entries $[c_{ik}]$ and D is an $f \times s$ matrix with entries $[d_{kj}]$. Hence,

$$CD = \begin{bmatrix} (n_1-1)\lambda_2 + \lambda_1 & n_1\lambda_2 & n_1\lambda_2 & ... & n_1\lambda_2 \\ n_2\lambda_2 & (n_2-1)\lambda_2 + \lambda_1 & n_2\lambda_2 & ... & n_2\lambda_2 \\ n_3\lambda_2 & n_3\lambda_2 & (n_3-1)\lambda_2 + \lambda_1 & ... & n_3\lambda_2 \\ ... & ... & ... & ... & ... \\ n_s\lambda_2 & n_s\lambda_2 & ... & ... & (n_s-1)\lambda_2 + \lambda_1 \end{bmatrix}$$

CD is illustrated as above. Now we apply elementary row and column operations. Firstly; for this purpose, we add -1 multiple of second column to first column. Then we add -1 multiple of third column to second column. We continue with this fashion till adding -1 multiple of sth column to $s-1$th column. Hence we have a matrix of

the form:

$$E = \begin{bmatrix} -\lambda_2+\lambda_1 & 0 & 0 & ... & n_1\lambda_2 \\ \lambda_2-\lambda_1 & -\lambda_2+\lambda_1 & 0 & ... & n_2\lambda_2 \\ 0 & \lambda_2-\lambda_1 & -\lambda_2+\lambda_1 & ... & n_3\lambda_2 \\ 0 & 0 & \lambda_2-\lambda_1 & ... & n_4\lambda_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & ... & (n_s-1)\lambda_2+\lambda_1 \end{bmatrix}$$

Moreover we apply elementary row operations to E. For this purpose, we add $+1$ multiple of first row to second row. Then we add $+1$ multiple of second row to third row. We continue with this fashion till adding $+1$ multiple of $s-1$th row to sth row and so we have a matrix of the form:

$$U = \begin{bmatrix} -\lambda_2+\lambda_1 & 0 & 0 & ... & n_1\lambda_2 \\ 0 & -\lambda_2+\lambda_1 & 0 & ... & (n_1+n_2)\lambda_2 \\ 0 & 0 & -\lambda_2+\lambda_1 & ... & (n_1+n_2+n_3)\lambda_2 \\ 0 & 0 & 0 & ... & (n_1+n_2+n_3+n_4)\lambda_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & ... & (n_1+n_2+...+n_{s-1}+n_s-1)\lambda_2+\lambda_1 \end{bmatrix}$$

As a result, we have an upper-triangle matrix U, and so $det(U)$ is the multiplication of diagonal entries. Our operations to CD do not affect the determinant, namely $det(CD) = det(U)$. Therefore $det(CD) = (\lambda_1-\lambda_2)^{s-1}(n_1+n_2+...+n_{s-1}+n_s-1)\lambda_2+\lambda_1$. Since $\sum_{i=1}^{s} n_i = v$, we have $det(CD) = (\lambda_1-\lambda_2)^{s-1}(\lambda_1-\lambda_2+v\lambda_2)$. We also note that $\lambda_1 > \lambda_2$. This implies that $det(CD) \neq 0$. Then CD is an $s \times s$ invertible matrix with rank s. For this reason $s \times f$ matrix C also has rank s. Thus $s \leq f$.

Remark 3.3.6. Let G consist of only identity element, 1. Then the number of orbits of G on $\mathcal{B}$ is $|\mathcal{B}| := b$ and the number of orbits of G on V is $|V| := v$. Hence $v \leq b$.

This result gives us one of the Fisher's inequality, which is stated in Theorem 3.2.6 in chapter 3.

(ii) Let G act transitively on both $\mathcal{B}$ and V. Also let $\alpha \in V$ and $B \in \mathcal{B}$. Then the rank of G acting on V is equal to the number of orbits of G_α acting on V by Definition 2.1.38. Similarly, the rank of G acting on $\mathcal{B}$ is equal to the number of orbits of G_B acting on $\mathcal{B}$.

Let m be the number of orbits of G acting on $V \times \mathcal{B}$. Since G acts transitively on $\mathcal{B}$ and V, m is equal to the number of orbits of G_α on V, say m_1, and to the number of orbits of G_B on $\mathcal{B}$, say m_2 by Definition 2.1.38. Thus m_1 is at most m and m_2 is at least m by part (i). □

Proposition 3.3.7. *Let G be an automorphism group of a Steiner system S and α be a point in S. Then G_α is an automorphism group of the one-point contraction of S, namely S_α.*

Proof. Let $S = S(V, \mathcal{B})$ and $\alpha \in V$. By Theorem 3.2.1, there exists a Steiner system $S_\alpha = S(V', \mathcal{B}')$, where $V' = V \setminus \{\alpha\}$ and $\mathcal{B}'$ is a family of blocks. In the process of contraction, we firstly exclude blocks not containing α. Later, we remove α from blocks containing α and get a new family of blocks $\mathcal{B}'$.

Let $g \in G_\alpha$ and also let $B \in \mathcal{B}$ such that $\alpha \in B$. Then $\alpha \in g(B)$ and $g(B)$ is a block in S. It follows that $g(B) \setminus \alpha$ is a block in S_α. Since g leaves α invariant, we have $g(B \setminus \alpha) = g(B) \setminus \alpha$. Therefore $G_\alpha \subseteq Aut(S_\alpha)$.

Let $h \in Aut(S_\alpha)$ and also let $B' \in \mathcal{B}'$. Then $h(B')$ is block in S_α. It follows that $B' \cup \alpha$ and $h(B') \cup \alpha$ are blocks in S. h leaves α invariant since α is not a point in S_α. This means that $h(B' \cup \alpha) = h(B')$. Thus $h \in G_\alpha$. Therefore $Aut(S_\alpha) \subseteq G_\alpha$.

Hence $G_\alpha = Aut(S_\alpha)$. □

Chapter 4

The construction of $S(5, 6, 12)$ by $S(2, 4, 13)$

This chapter is entirely based on the article of Hans Havlicek and Hanfried Lenz [19]. In this chapter, our construction of $S(5, 6, 12)$ is based on $S(2, 4, 13)$ that is a projective plane of order 3 by Theorem 3.2.7. Also I want to thank Hans Havlicek for allowing me to use his own figures in their article.

4.1 Introduction and definitions

Let $\mathcal{P}$ be the set of points of the projective plane of order 3; that is to say, $S(2, 4, 13)$. We know that there are exactly four lines (blocks) through each point of the projective plane of order 3 and each two lines have an intersection with exactly one point from Theorem 2.2.14. Also there are 13 points, and 13 lines, known as blocks, by the formula (3.1). The unique line joining distinct points A and B will be written AB.

Let α be fixed in $\mathcal{P}$. We will show that $W := \mathcal{P} \setminus \{\alpha\}$ together with a family $\mathcal{B}$ of subsets of six points is $S(5, 6, 12)$.

We start with the definitions that we will use throughout in this chapter.

Definition 4.1.1. A *triangle* is a set of three non-collinear points and three lines that are incident with two of them. We call points *vertices* and lines *sides*.

Remark 4.1.2. A side of a triangle in a projective plane is a line. On the other hand, a side of a triangle in a euclidean plane is a line segment, which is a part of a line bounded by two distinct points. Since closeness of points in a projective plane is not defined, line segment is not defined in a projective plane.

Definition 4.1.3. An *inscribed triangle* in the triangle T is a set of a three non-collinear points that separately lies on exactly one line of the triangle T

Definition 4.1.4. A *quadrangle* is a set of four points, no three of which are collinear, and a six lines that are incident with each pair of these points. The four points are called *vertices* and the six lines are called *sides* of the quadrangle.

Definition 4.1.5. Two sides of a quadrangle, say ℓ_1, ℓ_2 are *opposite* if the point that is incident with both lines is not a vertex of ℓ_1 and ℓ_2.

Definition 4.1.6. A *diagonal point* of a quadrangle is a point that is incident with opposite sides of the quadrangle.

Proposition 4.1.7. *A quadrangle has three diagonal points in a projective plane.*

Proof. Straightforward from using both Theorem 5.2.4 and Theorem 2.2.13. □

4.2 Classifying sets containing six points

In this section, we will show the classification of subsets of $\mathcal{P}$, each of which consists of six points since our aim is to discover sets of six points that are blocks of $S(5, 6, 12)$. We also note that figures of this section are illustrations of a projective plane of order 3.

Type 1. S is the union of a line and two additional points (Figure 4.1).

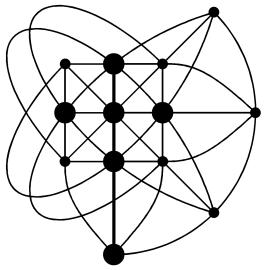

Figure 4.1

This set contains a line, which has four points. There are 13 options for the one line. Also, there are nine points that are not in the line, left for the two remaining points. So, there are $\binom{9}{2}$ options for the two additional points. In Figure 4.1, we illustrate a projective plane of order 3 and our example of choices for the one line and the two remaining points in the plane. In the figure, points depicted bold form a set of six points.

Hence, there are exactly $13 \cdot \binom{9}{2} = 13 \cdot 36$ sets of type 1.

Type 2. S is the symmetric difference of two different lines (Figure 4.2).

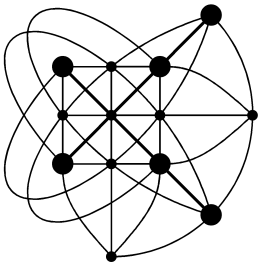

Figure 4.2

Since two different lines meet at exactly one point, their symmetric difference is the set of six points of two lines without the intersection point. We choose two lines out of thirteen lines. In Figure 4.2, we illustrate our example of choices for the two lines in the plane. In the figure, points depicted bold form a set of six points.

Hence, there are exactly $\binom{13}{2} = 13 \cdot 6$ sets of type 2.

Type 3. S consists of a triangle and an inscribed triangle (Figure 4.3).

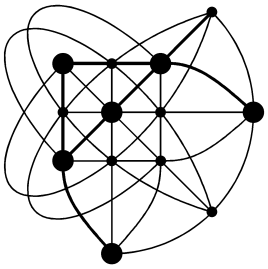

Figure 4.3

A triangle, so called main triangle, and an inscribed triangle, which is inscribed in the main triangle, have three vertices each. Then, vertices of each triangles form a set of six points S. Also, we note that each vertex of the inscribed triangle lies on exactly one line of the main triangle.

The main triangle has three lines that is incident with each pair of vertices. That is to say, each vertex of the main triangle is on exactly two lines. For counting the sets of type 3, we start with choosing the lines of a main triangle. Firstly, we choose one line out of thirteen lines. There are 13 options for this line. We want to select a second line, and so there are 12 options for that. These two lines that we have chosen have an intersection at only one point. We know that there are four lines through that point. Since we want to choose a line that does not intersect the previous two lines that we have chosen at the common point, there are $\binom{9}{1}$ options for the third line. Therefore, we have chosen three lines for forming the main triangle

Moreover, we need to avoid repetitions because the order of choosing does not matter. For this reason, we divide $\binom{13}{1}\binom{12}{1}\binom{9}{1}$ by 3! for counting the number of ways to form the main triangle.

Now, we have to choose the vertices of the inscribed triangle. What we know about the vertices is that these must be non-collinear points that lie on exactly one line of the main triangle each. Then, we have three lines and there are two vertices of the main triangle in each line. So there are two possible vertices in each line for the inscribed triangle.

Let us pick a one line out of three lines of the main triangle. There are two options for the vertex of the inscribed triangle. Then, there are $\binom{3}{1} \cdot 2$ options for the first vertex. Further, we pick the second line out of two lines. Then, there are two options for the second vertex of the inscribed triangle, and so there are $\binom{2}{1} \cdot 2$ options for the second vertex.

Finally, when we pick the last line of the main triangle, there is only one option for the last vertex on the last line since the other two vertices of the inscribed triangle decides the line that intersects at exactly one point of the last line. If we exclude the two vertices of the main triangle and the intersection point, which violates the

non-collinearity condition for the inscribed triangle, on the last line, we have only one option for the remaining vertex of the inscribed triangle.

In Figure 4.3, we illustrate our example of the main triangle and the inscribed triangle. In the figure, points depicted bold form a set of six points and lines depicted bold are the sides of the main triangle.

Since the order of choice is not important, we divide $\binom{3}{1} \cdot 2 \cdot \binom{2}{1} \cdot 2$ by 3!.

Hence, there are exactly $\frac{\binom{13}{1}\binom{12}{1}\binom{9}{1}}{3!} \cdot \frac{\binom{3}{1}2\binom{2}{1}2}{3!} = 13 \cdot 72$ sets of type 3.

Type 4. S is the set of vertices of quadrangle and two of its diagonal points (Figure 4.4).

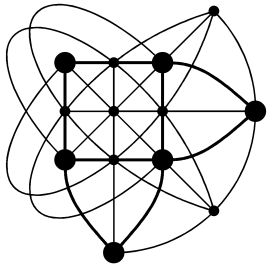

Figure 4.4

A quadrangle has four vertices, no three of which are collinear, and three diagonal points. Our proceeding will be similar to type 3. That is, we will start picking lines. We will have chosen four lines at the end.

First we choose one line out of thirteen lines, and so there are $\binom{13}{1}$ options. Then, we choose a second line out of twelve lines. There are $\binom{12}{1}$ options. These two lines that we have picked intersects in only one point. We know that there are four lines

through that intersection point. Hence, we exclude these lines for choosing the third line. Hence, there are $\binom{9}{1}$ options for the third line.

Finally, we pick a fourth line that does not intersect previous three lines that we have picked at common points of each of these lines between them since we want to yield the four vertices of the quadrangle. We have already picked three lines, say ℓ_1, ℓ_2, ℓ_3. Let us call c_1 the common point of ℓ_1 and ℓ_2, c_2 of ℓ_2 and ℓ_3, c_3 of l_1 and l_3. There are four lines through c_1 and c_2 each. Also, ℓ_2 is the common line through c_1 and c_2. Hence, there are seven lines through c_1 or c_2. Likewise, there are four lines through c_3. Since ℓ_1 and ℓ_3 are the common lines through c_3, there are nine lines through one of c_1, c_2 or c_3. Hence, there are 4 options for the fourth line.

In Figure 4.4, we illustrate our example of the quadrangle. In the figure, points depicted bold form a set of six points and lines depicted bold are the sides of the quadrangle.

Also, we need to avoid repetitions since the order does not matter. For this reason, we divide $\binom{13}{1}\binom{12}{1}\binom{9}{1}\binom{4}{1}$ by 4!.

Hence, there are exactly $\frac{\binom{13}{1}\binom{12}{1}\binom{9}{1}\binom{4}{1}}{4!} = 13 \cdot 18$ sets of type 4.

Now, we will show that the four types are disjoint with each other.

Type 1 and Type 2

We suppose that there exists a set S of six points that belongs to both type 1 and type 2. Then, S is the union of a line, say ℓ_1, and two additional points, say A and B. Since also S is the symmetric difference of two different lines, there is a line, say ℓ_2, through A and B and so the symmetric difference of ℓ_1 and ℓ_2 will exclude a point, say C, lies on ℓ_1 and ℓ_2 from the set S. However, C is in union of a line and two additional points A and B. Therefore, we get a contradiction; so type 1 and

type 2 are disjoint.

Type 1 and Type 3

We suppose that there exists a set S of six points that belongs to both type 1 and type 3. Then, S consists of a triangle with the set of vertices $\{E, F, G\}$ and an inscribed triangle with the set of vertices $\{P, Q, R\}$ with $P \in FG$, $R \in EF$ and $Q \in EG$. Also, S is the union of a line and two further points.

Suppose the line FG has four points from the set S of six points, without loss of generality. We know that $P \in FG$ so we need to find one more point in FG. But $E \notin FG$ because the points E, F, G are non-collinear. In addition, $Q \notin FG$ because Q lies in EG and G is the only intersection point of the lines EG and FG. Similarly, $R \notin FG$ because R lies in EF and F is the only intersection point of the lines EF and FG. Therefore, we get a contradiction; so type 1 and type 3 are disjoint.

Type 1 and Type 4

We suppose that there exists a set S of six points that belongs to both type 1 and type 4. Then, S is the set of vertices of the quadrangle $\{A, B, C, D\}$ and two diagonal points $\{E, F\}$ with $E \in AD \cap BC$ and $F \in AB \cap CD$. Also, S is the union of a line and two additional points.

Without loss of generality; suppose the line AD has four points from the set S of six points. We know that $E \in AD$ so we need to find one more point in AD. But B and C are not in AD since AD and BC have a common point E, which is a diagonal point, make AD and BC opposite sides of the quadrangle. Also, F can not be in AD since it is the other diagonal point. Therefore, we get a contradiction; so type 1 and type 4 are disjoint.

Type 2 and Type 3

We suppose that there exists a set S of six points that belongs to both type 2 and type 3. Then S consists of a triangle with the set of vertices $\{E, F, G\}$ and an inscribed triangle with the set of vertices $\{P, Q, R\}$ with $P \in FG$, $R \in EF$ and $Q \in EG$.

Also, S is the symmetric difference of two different lines, say a and b. Therefore, the set S of six points lie in a and b. Let us say; for the triangle $\{E, F, G\}$, two of its points lie on a. Also a and b have a common point, say U, which is not in S. There is a one point remaining that lies on a, which is the one of the vertices $\{P, Q, R\}$ of the inscribed triangle. As a result, two of the vertices of the inscribed triangle lies on b, and also one of the vertices $\{E, F, G\}$ of the triangle lies on b.

Without loss of generality; let us say E and F lie on a and P and Q lie on b. Hence, G must lie in b; but $G \notin b$ since b is uniquely determined by two distinct points P and Q. Therefore, we get a contradiction; so type 2 and type 3 are disjoint.

Type 2 and Type 4

We suppose that there exists a set S of six points that belongs to both type 2 and type 4. Then S is the set of vertices of quadrangle $\{A, B, C, D\}$ and two diagonal points $\{E, F\}$ with $E \in AD \cap BC$, $F \in AB \cap CD$. Also, S is the symmetric difference of two different lines, say a and b.

Since any three of vertices of the quadrangle must be non-collinear, without loss of generality; let us say A and B lie on a and C and D lie on b. Then, $F \in AB \cap CD$ will be excluded by the symmetric difference. Therefore, we get a contradiction; so type 2 and type 4 are disjoint.

Type 3 and Type 4

We suppose that there exists a set S of six points that belongs to both type 3 and

type 4. Then S is the set of vertices of quadrangle $\{A, B, C, D\}$ and two diagonal points $\{E, F\}$ with $E \in AD \cap BC$, $F \in AB \cap CD$. Also S consists of a triangle and an inscribed triangle.

AD and BC are the opposite sides of the quadrangle since these lines meet at the diagonal point E. The line CD intersects these lines at the points C and D. Since C, D and E are non-collinear, the lines AD, BC and CD form a triangle. Furthermore, the remaining three points $\{A, B, F\}$ lie in same line; hence, we can not form a second triangle. Therefore, we get a contradiction; so type 3 and type 4 are disjoint.

In conclusion, these four types of sets of six points are distinct with each other. We have $13 \cdot (36 + 6 + 72 + 18) = 13 \cdot 132 = 1716$ sets of six points in total. As $\binom{13}{6} = 1716$, our list contains all possible sets.

4.3 Construction of $S(5, 6, 12)$

We want to form $S(5, 6, 12)$. For this purpose, we need to have a set W of 12 points together with a family of subsets of 6 points in W.

Let α be fixed in $\mathcal{P}$ and let us define $W := \mathcal{P} \setminus \{\alpha\}$. A block B is defined to be a subset of W satisfying one of the following conditions.

i. B is the symmetric difference of two distinct lines, neither containing α.

Since neither line is incident with α and there are four lines through α, there are 9 options for the first line. For the second line, there are 8 options.

If repetitions are taken into account, there are $\frac{\binom{9}{1}\binom{8}{1}}{2!} = 36$ blocks of class i.

ii. $B \cup \{\alpha\}$ is the union of two distinct lines.

Firstly, α may be on both lines. Since there are four lines through α, we will pick two lines out of four lines. Hence, we have $\binom{4}{2} = 6$ blocks of class *ii*.

Secondly, α may not be on both lines; but at least one line has α. There are four lines that are incident with α. Then, we have four options for the line through α. For the second line, we have nine options. Hence, we have $4 \cdot (13 - 4) = 36$ blocks of class *ii*.

Finally, if α is not on both lines, the union $B \cup \{\alpha\}$ will be the set of seven points; however, we want to form sets of six points. Hence, there are 42 blocks of class *ii*.

iii. B consists of a quadrangle with two of its diagonal points. Also, α is the remaining diagonal point.

We take two distinct lines, say A and B, through α. Then, there are $\binom{4}{2} = 6$ options. Also, we will choose two distinct points on $A \setminus \{\alpha\}$ and $B \setminus \{\alpha\}$, respectively. Hence, there are $\binom{3}{2}\binom{3}{2}$ options. Since α is excluded, two diagonal points are left; and so we have only one option for picking diagonal points.

Therefore, we have $\binom{4}{2}\binom{3}{2}\binom{3}{2} = 54$ blocks of class *iii*.

To sum up, we have a total of $36 + 42 + 54 = 132$ blocks.

Now, we have to prove that the set W together with the set of 132 blocks is $S(5, 6, 12)$. In the next theorem, we will prove that.

Here is the main result of this chapter.

Theorem 4.3.1. [19, Theorem 1] *The set W, together with the set of all blocks, is $S(5, 6, 12)$.*

Proof. First we note that the number of points in W is 12 and all blocks have exactly 6 points.

Second we will show that for each set M of five points in W belongs to at least one block. We consider $S := M \cup \{\alpha\}$ as a set of six points. Then there are four cases depending on the types of the sets of six points.

1. Suppose that S is a set of type 1, consists of a line a and two additional points. Let b be the line joining these two points. Then $(a \cup b) \setminus \{\alpha\}$ is a block of class ii containing M.

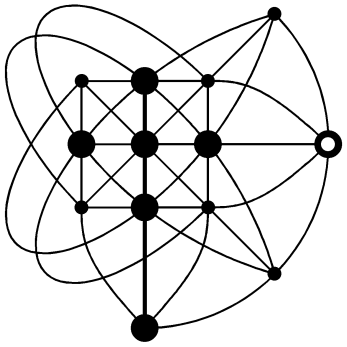

Figure 4.5

In Figure 4.5, we illustrate an example of a set of type 1. In the figure, points depicted bold form a set of six points and ring-shaped point is α.

2. Let S be a set of type 2, the symmetric difference of two distinct lines. Let a and b be our two distinct lines. Then $(a \cup b) \setminus \{\alpha\}$ is a block of class ii containing M.

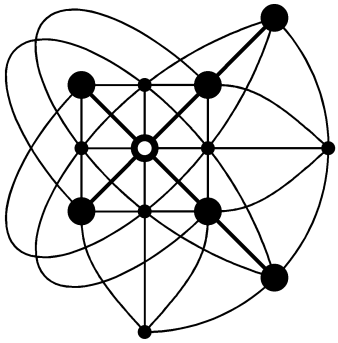

Figure 4.6

In Figure 4.6, we illustrate an example of a set of type 2. Bold-lines are our lines a and b and α is the common point of these lines. By the symmetric difference of a and b, α is excluded and can be seen as ring-shaped point in the figure.

3. Let S be a set of type 3, consists of a triangle with the set of vertices $\{A, B, C\}$ and an inscribed triangle with the set of vertices $\{P, Q, R\}$ with $P \in BC$, $R \in AB$ and $Q \in AC$.

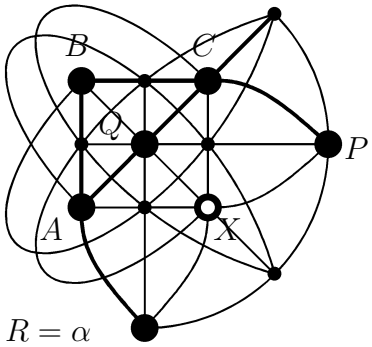

Figure 4.7

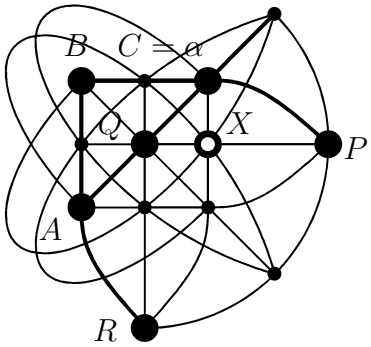

Figure 4.8

Now, we have to consider two cases for α: if α is in $\{P, Q, R\}$, let $R = \alpha$ without loss of generality, and define the point $X := AP \cap BQ$. X can be seen as ring-shaped point in Figure 4.7. Then $X \in CR$ and the set of points $\{A, B, C, X\}$ is the vertices of a quadrangle with diagonal points Q and P. Also $R = \alpha$. Hence the set $\{A, B, C, X, Q, P\}$ is exactly the block of class *iii* containing M.

Otherwise, α is not in $\{P, Q, R\}$. Let $C = \alpha$ without loss of generality, and define the point $X := PQ \cap BQ$. X can be seen as ring-shaped point in Figure 4.8. Then it follows that $X \in AB \cup PQ$. Hence the symmetric difference of AB and PQ is a block of class i containing M.

4. Let $S = \{A, B, C, D, E, F\}$ be the set of vertices of the quadrangle and two diagonal points, so called type 4.

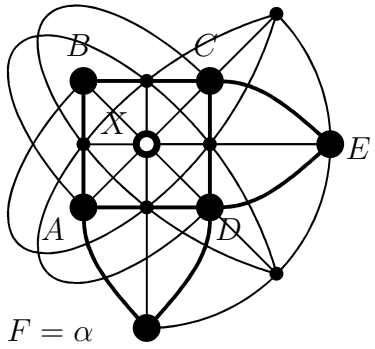

Figure 4.9

Without loss of generality, let $\alpha = F = AB \cap CD$ in Figure 4.9. This means that $\{A, B, C, D\}$ is the set of vertices of the quadrangle with two diagonal points E and α. Let X be the third diagonal point of the quadrangle that can be seen as ring-shaped point in the figure. Hence the set $\{A, B, C, D, E, X\}$ is the block of class *iii* containing M.

Finally, we will compute the number of blocks containing our set M of five points. Each of the 132 blocks contains exactly $\binom{6}{5} = 6$ subsets of five points. Then we have $132 \cdot 6 = 792$ sets of five points in total. Previously, we have shown that any set M of five points is contained in at least one block; and so it follows that the number of blocks is greater than or equal to 1 for each $\binom{12}{5} = 792$ possible sets M. Hence, the number of blocks is equal to 1 for all M. $\square$

Chapter 5

The construction of $S(5, 6, 12)$ by $S(2, 3, 9)$

In this chapter, we will form a Steiner system of type $S(5, 6, 12)$ by using the 3-fold extension of $S(2, 3, 9)$. Our work is based on John D. Dixon and Brian Mortimer's book [16] *Permutation Groups*. In chapter 4, our construction of $S(5, 6, 12)$ is based on $S(2, 4, 13)$ that is a projective plane of order 3 by Theorem 3.2.7. On the other hand, in this chapter, our construction of $S(5, 6, 12)$ is based on $S(2, 3, 9)$ that is an affine plane of order 3 by Theorem 3.2.8. For this reason, we presume some familiarities with an affine plane of order 3 in this chapter.

5.1 The one-point extension of $S(2, 3, 9)$

First what we mean by the one-point extension of a Steiner system of type $S(t, k, v)$ is to increase the parameters one point more to have $S(t + 1, k + 1, v + 1)$. Then we have to sure that $S(t + 1, k + 1, v + 1)$ really exists. In this section, we will extend

$S(2,3,9)$ to $S(3,4,10)$ by adding one point and show that $S(3,4,10)$ exists. We start showing the uniqueness of $S(2,3,9)$ up to isomorphism.

Theorem 5.1.1. *There is a unique $S(2,3,9)$ Steiner system up to isomorphism.*

Proof. Let S be any Steiner system of type $S(2,3,9)$. Since $S(2,3,9)$ is an affine plane by Theorem 3.2.8, we call blocks of S lines, which are incident with three points. Moreover, the lines of S can be partitioned into four parallel classes and each parallel class has three lines by Theorem 2.2.11. Now, let us choose one parallel class, say P_1, and write down its lines, namely ℓ_1, ℓ_2, ℓ_3 as three columns. Then we have displayed all nine points of an affine plane in the columns.

Let ℓ_4 be a line that is not parallel to the lines of P_1. Then ℓ_4 contains exactly one point in each lines ℓ_1, ℓ_2 and ℓ_3. By Definition 2.2.6, for every point x in the plane and the line ℓ_4 not through x, there exists a unique line through x that does not meet ℓ_4. Since there are six points that are not in ℓ_4, we can form two lines ℓ_5 and ℓ_6 that are parallel to ℓ_4. Hence, we have formed a second parallel class, say P_2.

Let ℓ_7 be a line that is non-parallel to the lines of P_1 and P_2. When we apply our previous reasoning to ℓ_7, we can form two lines ℓ_8 and ℓ_9 which are parallel to ℓ_7. Hence, we have formed a second parallel class, say P_3.

Our final fourth parallel class, say P_4, will be formed with same previous procedure. In short, we show that parallel classes of $S(2,3,9)$ is formed in exactly one way. Therefore, there is a unique $S(2,3,9)$. □

Now, we will show the one-point extension of the Steiner system of type $S(2,3,9)$. First we assume that we already have an $S(3,4,10)$. Also, we know that if $S(t,k,v)$ exists then $S(t-1,k-1,v-1)$ exists from Theorem 3.2.1. Therefore, if we remove a point, say α, from $S(3,4,10)$ then we will have $S(2,3,9)$. For this reason, a block in

$S(3,4,10)$ containing α is of the form $\Omega \cup \{\alpha\}$ where Ω denotes a block in $S(2,3,9)$. Since there are 12 blocks in $S(2,3,9)$ by the formula (3.1), we have 12 sets of form $\Omega \cup \{\alpha\}$.

We observe that $\Omega \cup \{\alpha\}$ has three collinear points and α. Also, we recall that the number of blocks in an $S(t,k,v)$ is $\frac{\binom{v}{t}}{\binom{k}{t}}$ (3.1). As a result, the number of blocks in an $S(3,4,10)$ is $\frac{\binom{10}{3}}{\binom{4}{3}} = 30$. We have already counted 12 blocks which are of the form $\Omega \cup \{\alpha\}$. Then there are 18 blocks that do not contain α or any three collinear points. These blocks have four points from $S(2,3,9)$, no three are collinear. We will call these sets of four points quadrangles.

In $S(2,3,9)$, there are $\binom{9}{4} = 126$ sets of four points in total. Now, we want to exclude sets that have three collinear points. Recall that there are twelve lines. Hence, we pick a one line in 12 different ways. Also, we choose a one further point out of six points those are not in the line that we have picked. Consequently, there are $\binom{12}{1}\binom{6}{1} = 72$ sets of four points containing three collinear points. Then, the number of quadrangles is $126 - 72 = 54$.

Definition 5.1.2. Two sides of a quadrangle are *opposite* if these lines are parallel to each other.

We know that there are four parallel classes for lines, and so six lines of a quadrangle belong to one of the four parallel classes. There are two pairs of the opposite lines that provide us a four vertices of a quadrangle in their intersections. Hence, we can relate to each quadrangle a pair $\{x,y\}$ where x and y are those parallel classes that contain such a pair.

Let us denote the set of four parallel classes of $S(2,3,9)$ by a,b,c,d. The set $\{a,b,c,d\}$ can be partitioned in three different ways into a pair of sets of two points: $\{a,b\} \mid \{c,d\}$, $\{a,c\} \mid \{b,d\}$ and $\{a,d\} \mid \{b,c\}$. Then we assign each partition to the sets S_i as follows:

(*i*) S_1 := the set of quadrangles with the partition $\{a, b\} \mid \{c, d\}$.

(*ii*) S_2 := the set of quadrangles with the partition $\{a, c\} \mid \{b, d\}$.

(*iii*) S_3 := the set of quadrangles with the partition $\{a, d\} \mid \{b, c\}$.

Proposition 5.1.3. *The automorphism group of* $S(2, 3, 9)$ *acts transitively on the set of* 4 *parallel classes,* $\{a, b, c, d\}$.

Proof. We know that $S(2, 3, 9)$ is an affine plane from Theorem 3.2.8. Then the points of $S(2, 3, 9)$ is the set $\mathbb{F}_3^2 = \{(0, 0), (1, 0), (2, 0), (0, 1), (1, 1), (2, 1), (0, 2), (1, 2), (2, 2)\}$. Each parallel class partition the nine points of $S(2, 3, 9)$. Let a and b be two parallel classes of $S(2, 3, 9)$ and also let $\ell_1 \in a$ and $\ell_1^{'} \in b$. Since automorphisms of $S(2, 3, 9)$ send an affine subspace to an affine subspace, there exists an automorphism g such that $g(\ell_1) = \ell_1^{'}$. Then let ℓ_2 and ℓ_3 be other two lines in a. Since g is not an identity map, we have $g(\ell_2) \neq \ell_2$ and $g(\ell_3) \neq \ell_3$. Moreover, we have $g(\ell_2) \neq \ell_3$ and $g(\ell_3) \neq \ell_2$ since $\ell_1^{'} \notin a$. Also g can not send ℓ_2 to the parallel classes c or d since there is no common point of ℓ_1 and ℓ_2. Hence g sends ℓ_2 and ℓ_3 to the remaining lines of the parallel class b so that $g(\ell_1), g(\ell_2)$ and $g(\ell_3)$ contains all nine points of $\mathbb{F}_3^2$. Therefore $Aut(S(2, 3, 9))$ acts transitively on the set of parallel classes. □

Since the automorphism group of $S(2, 3, 9)$ acts transitively on the set of parallel classes, each of these sets contains 18 quadrangles of the 54 quadrangles of $S(2, 3, 9)$. In the next theorem we will show that each triangle of $S(2, 3, 9)$ is contained in a unique quadrangle from each set S_i for $i = 1, 2, 3$.

Theorem 5.1.4. [16, Theorem 6.3B.] *Each set* $S = S_i (i = 1, 2, 3)$ *has the property that each triangle of* $S(2, 3, 9)$ *is in a unique quadrangle from each set. For the converse,* S_1, S_2 *and* S_3 *are the only sets of* 18 *quadrangles with this property.*

Proof. In each quadrangle, we can form four different triangles since any three of

four points of a quadrangle are non-collinear, and so there are $\binom{4}{3} = 4$ options for having a triangle in a quadrangle. In $S(2, 3, 9)$, there are $\binom{9}{3} = 84$ sets of three points in total. Then if we exclude sets of three collinear points, which are the twelve lines, we have $84 - 12 = 72$ sets of three non-collinear points, so triangles. We will show that each triangle is in unique quadrangle from each set S_i. In other words, we will show that the 18 quadrangles from each set S_i cover $18 \cdot 4 = 72$ triangles of $S(2, 3, 9)$.

Due to the symmetry of the partition of the parallel classes, we will contemplate only one S_i to prove each triangle is in a unique quadrangle. We choose S_1, the set of quadrangles with the partition $\{a, b\} \mid \{c, d\}$, without loss of generality. Let T be any triangle. Since T is made up by 3 non-collinear points, three sides of T are in different parallel classes. Then one parallel class, say d, is not represented in T.

We add a point, say π, to T in order to obtain a quadrangle. There are three lines through the point π, and these lines lie in different parallel classes. Then d is represented in the one of three lines through π. As a result, T is not contained in a quadrangle with a parallel class pair $\{c, d\}$.

Thus T is contained in a quadrangle with a parallel class pair $\{a, b\}$. We will show that this quadrangle is unique. Assume to the contrary, there exist quadrangles Ξ_1 and Ξ_2 containing T. Hence three vertices of these quadrangles are the same due to T. Then the fourth vertex of the Ξ_1 and Ξ_2 is different, say π_1 in Ξ_1 and π_2 in Ξ_2. Also, let us say the vertices of T as v_1, v_2, v_3. We assume that the line through v_1 and v_2 is in the class of a, and the line through v_2 and v_3 is in the class of b without loss of generality. There is a line in the class of a through v_3 and a line in the class of b through v_1. Since these two lines are not parallel, these intersect at π_1 and π_2. Then we have $\pi_1 = \pi_2$ and so we get a contradiction. Consequently, T is contained in a unique quadrangle.

Conversely, we will prove that $S_i (i = 1, 2, 3)$ are the only sets of 18 quadrangles

with this property. We suppose that S is a set of 18 quadrangles such that each triangle of $S(2,3,9)$ is in a unique quadrangle from S. Let q_1 and q_2 be a points in the $S(2,3,9)$. We define a set Q consisting of quadrangles which contain these points.

If the line through q_1 and q_2 has a parallel pair in the quadrangle, then we have two options left for the pair since a parallel class has three lines. Also, for the second parallel pair we have three options since there are four parallel class in total. Thus we can form $2 \cdot 3 = 6$ different quadrangles. If the line through q_1 and q_2 does not have a parallel pair in the quadrangle, then we have three options left for the second line that does not have a parallel pair since there are three parallel class left for the second line. Thus we can form 3 different quadrangles. Hence in total we have $6 + 3 = 9$ quadrangles in Q.

The number of triangles containing q_1 and q_2 in $S(2,3,9)$ is six since we exclude one point that lies in same line with q_1 and q_2, and so for the third vertex we have six possible points. We know that a quadrangle has four triangles in it. Also each triangle is in a unique quadrangle.

Previously we have shown that there are nine quadrangles containing q_1 and q_2. In each quadrangle, there are uniquely represented two triangles containing these points. However we do not have $2 \cdot 9 = 18$ triangles. Therefore we can partition nine quadrangles into three sets those have three quadrangles consisting of all six triangles in $S(2,3,9)$. □

Finally, we have shown 18 blocks that do not contain α or any three collinear points of $S(2,3,9)$. As a result, $S(3,4,10)$ exists.

5.2 The one-point extension of $S(3, 4, 10)$

In this section, we will extend $S(3, 4, 10)$ to $S(4, 5, 11)$ by adding one point and show that $S(4, 5, 11)$ exists. We start showing the uniqueness of $S(3, 4, 10)$ up to isomorphism.

Theorem 5.2.1. *There is a unique $S(3, 4, 10)$ up to isomorphism.*

Proof. Let $\{a, b, c, d\}$ be the set of parallel classes of $S(2, 3, 9)$. In the previous section, we see that the set $\{a, b, c, d\}$ can be partitioned in three different ways into a pair of sets of two points: $\{a, b\} \mid \{c, d\}$, $\{a, c\} \mid \{b, d\}$ and $\{a, d\} \mid \{b, c\}$. Let the set $\{a, b, c, d\}$ be ordered. By Proposition 5.1.3, $Aut(S(2, 3, 9))$ acts transitively on $\{a, b, c, d\}$. Then there exists $g_1 \in Aut(S(2, 3, 9))$ such that $g_1(\{a, b, c, d\}) = \{a, c, b, d\}$. Also there exists $g_2 \in Aut(S(2, 3, 9))$ such that $g_2(\{a, b, c, d\}) = \{a, d, b, c\}$. Therefore $Aut(S(2, 3, 9))$ acts transitively on $X = \{\{a, b\} \mid \{c, d\}, \{a, c\} \mid \{b, d\}, \{a, d\} \mid \{b, c\}\}$.

We have formed $S(3, 4, 10)$ by adding a point α to $S(2, 3, 9)$ in the previous section. Recall that we define sets $S_1 :=$ the set of quadrangles with the partition $\{a, b\} \mid \{c, d\}$, $S_2 :=$ the set of quadrangles with the partition $\{a, c\} \mid \{b, d\}$ and $S_3 :=$ the set of quadrangles with the partition $\{a, d\} \mid \{b, c\}$. By Theorem 5.1.4, 18 blocks that do not contain α can be picked one of the S_1, S_2 or S_3. Since $Aut(S(2, 3, 9))$ acts transitively on X, it also acts transitively on $\{S_1, S_2, S_3\}$. Hence where we take 18 blocks does not matter. Therefore $S(3, 4, 10)$ is unique up to isomorphism. □

Now, we will show the one-point extension of $S(3, 4, 10)$ in order to obtain $S(4, 5, 11)$. As in the previous section, we assume that we already have an $S(4, 5, 11)$. Let us pick two points α and β in $S(4, 5, 11)$. If we remove α from $S(4, 5, 11)$ we have $S(3, 4, 10)$. In a same manner, if we remove β from $S(4, 5, 11)$ we have $S(3, 4, 10)$. Since $S(3, 4, 10)$ is unique up to isomorphism by Theorem 5.2.1, the contractions

of $S(4,5,11)$ due to α and β are isomorphic. Also these are one-point extension of $S(2,3,9)$. Thus we can say that the set of points of $S(4,5,11)$ consists of points of $S(2,3,9)$, α and β.

Hence the blocks of $S(4,5,11)$ containing α or β or both are the following forms:

(i) $\Omega \cup \{\alpha, \beta\}$

In this type of block, Ω is a block (line) of $S(2,3,9)$. Since there are 12 such Ω, we have 12 such form of $\Omega \ \cup \ \{\alpha, \beta\}$.

(ii) $\Xi \cup \{\alpha\}$

In this type of block, Ξ is a quadrangle from S_i that is defined in the previous section. Since there are 18 such Ξ in S_i, we have 18 such form of $\Xi \cup \{\alpha\}$. Without loss of generality we pick S_1 for Ξ to obtain $\Xi \cup \{\alpha\}$.

(iii) $\Xi \cup \{\beta\}$

In this type of block, Ξ is a quadrangle from S_i that is defined in the previous section. Since there are 18 such Ξ in S_i, we have 18 such form of $\Xi \cup \{\beta\}$. Without loss of generality we pick S_2 for Ξ to obtain $\Xi \cup \{\beta\}$.

Again, we recall that the number of blocks in an $S(t,k,v)$ is $\frac{\binom{v}{t}}{\binom{k}{t}}$ (3.1). As a result, the number of blocks in an $S(4,5,11)$ is $\frac{\binom{11}{4}}{\binom{5}{4}} = 66$. We have already shown $12 + 18 + 18 = 48$ blocks. We will look for remaining blocks that contain neither α nor β. That is to say, remaining blocks are made by five points from $S(2,3,9)$. For this reason, we firstly prove some properties of $S(2,3,9)$, which is an affine plane, for our further purpose. Readers may check Section 2.2.2 in chapter 2 for background knowledge for an affine plane in the proofs of four lemmas below.

Lemma 5.2.2. *Any set of five points in $S(2,3,9)$ contains at least one line.*

Proof. Assume to the contrary, there exists a set K of five points that does not contain a line. That is, a line that is incident with any two points in K does not contain a third point in K. Thus there are $\binom{5}{2} = 10$ different lines that are incident with two points of K. Hence there must be ten points which are not in K. However there are only four points that are not in K. Therefore we get a contradiction. □

Lemma 5.2.3. *Any set of five points in $S(2, 3, 9)$ contains a quadrangle.*

Proof. Let us choose any five points, say x_1, x_2, x_3, x_4, x_5. Then without loss of generality we pick x_1, x_2 to connect these with a line, say ℓ_1. Then one of the remaining three points, x_3, x_4, x_5, will lie in ℓ_1 by the previous lemma.

We suppose that x_3 lies in ℓ_1 without loss of generality. Then there exist a line, say ℓ_2, through x_4 that is parallel to ℓ_1 and a line, say ℓ_3, through x_5 that is parallel to ℓ_1. First we assume that $\ell_2 = \ell_3$. We want to connect x_4 with a point from ℓ_1, without loss of generality say x_1. Thus there exists a line, say ℓ_4, through x_1 and x_4. Also there exists a line, say ℓ_5, through x_1 and x_5. We want to connect x_5 with one more point, say x_2, without loss of generality. Then there exists a line, say ℓ_6, through x_2 and x_5. Also there exists a line, say ℓ_7, through x_2 and x_4.

Hence we have six lines connecting each pair of four points. There are two lines, ℓ_4, ℓ_5, through x_1. Also there are two lines, ℓ_6, ℓ_7, through x_2. In addition to these, ℓ_4 and ℓ_5 are in different parallel classes, and ℓ_6 and ℓ_7 are in different parallel classes.

Since ℓ_1 and ℓ_2 are in same parallel class, say a, $\ell_4, \ell_5, \ell_6, \ell_7$ represent remaining three parallel classes, say b, c, d. Let us say ℓ_4 is in b. Then ℓ_5 must be in c or d. Let us suppose ℓ_5 is in c. Since ℓ_6 and ℓ_7 are in different parallel classes, one of them will lie in b or c. Therefore we see that one more parallel class, say c, that have two lines.

Hence we have a quadrangle with a parallel class pair $\{a, c\}$. □

Lemma 5.2.4. *For any quadrangle Ξ in $S(2,3,9)$, there is a unique point δ not in Ξ that lies on two distinct lines of Ξ.*

Proof. Let Ξ be a quadrangle. Without loss of generality, we assume that Ξ has a parallel class pair $\{a,b\}$. We note that there are six lines that contain each pair of vertices of Ξ. Four lines are counted in a pair $\{a,b\}$.

Then there are two lines, say ℓ_1, ℓ_2, that are in different parallel classes, namely c and d. Therefore, ℓ_1 and ℓ_2 have a point in common, say δ. Also δ is not a vertex of Ξ since the four vertices of a quadrangle lie in intersections of lines in a pair $\{a,b\}$. Hence δ is not in Ξ. In addition to this, δ is unique point outside of Ξ since lines in a pair $\{a,b\}$ meet at vertices of Ξ. □

Remark 5.2.5. The point δ is called the diagonal point of the quadrangle.

Lemma 5.2.6. *For any quadrangle Ξ in the $S(2,3,9)$, there exists a unique quadrangle Ξ^* disjoint from Ξ, and Ξ and Ξ^* have the same diagonal point.*

Proof. Let Ξ be a quadrangle with a parallel class pair $\{a,b\}$ without loss of generality. We note that in the $S(2,3,9)$ there are 12 distinct lines. Then Ξ has 6 lines by the definition of a quadrangle. Thus there are 6 lines that are not in Ξ.

Also there are five points that lie outside of Ξ. By Lemma 5.2.3, a set of five points contains a quadrangle. Hence there exists a quadrangle, say Ξ^*. Then Ξ^* has also 6 lines, which means these are the remaining 6 lines that are not in Ξ. Therefore Ξ^* is a unique quadrangle.

Let δ be the diagonal point of Ξ. Thus δ is one of the five points that lie outside of Ξ. Since there are four lines through a point in $S(2,3,9)$, there are four lines through δ. Two lines that are incident with δ are lines of Ξ. Since Ξ is a quadrangle with a parallel class pair $\{a,b\}$, these lines are in parallel classes c and d separately.

Then the remaining lines, which are lines of Ξ^*, will be in parallel classes a and b separately.

We suppose that δ is a vertex of Ξ^*. Then Ξ^* is a quadrangle with a parallel class pair $\{a, b\}$. However there are only three lines in each parallel class and Ξ is also a quadrangle with a parallel class pair $\{a, b\}$. This violates the disjointness between Ξ and Ξ^*. Therefore we get a contradiction, so δ is not a vertex of Ξ^*.

Moreover, since δ lies in two distinct lines from different parallel classes, namely a and b, the other four points, which are vertices of Ξ^*, lie in these lines. Therefore δ is a diagonal point of Ξ^*. □

In the proof of Lemma 5.2.6, we have also proven the corollaries below.

Corollary 5.2.6.1. *If Ξ has a pair $\{a, b\}$ then Ξ^* has a pair $\{c, d\}$.*

Corollary 5.2.6.2. *Any set of five points that is disjoint from a quadrangle in $S(2, 3, 9)$ lies in exactly two distinct lines that have an intersection.*

Now, we return our mission of finding the blocks of $S(4, 5, 11)$. We look for blocks that have neither α or β. In other words, we look for the blocks that are made of five points from $S(2, 3, 9)$.

We have shown that any set of five points in $S(2, 3, 9)$ contains a quadrangle in Lemma 5.2.3. The previous blocks that we have shown contains quadrangle from S_1 and S_2. Since every set of four points is in a unique block due to the definition of a Steiner system of type $S(4, 5, 11)$, the remaining blocks that we have looked for contain a quadrangle from S_3. From Lemma 5.2.4. we know that any quadrangle Ξ from S_3 will have a unique point δ, which is a diagonal point of Ξ. Hence the last type of block is the following form:

(iv) $\Xi \cup \{\delta\}$

In this type of block, Ξ is a quadrangle from S_3 that is defined in the previous section. Since there are 18 such Ξ in S_3, we have 18 such form of $\Xi \cup \{\delta\}$.

Finally, we have shown 18 blocks that do not contain neither α nor β. Therefore $S(4, 5, 11)$ exists.

5.3 The one-point extension of $S(4, 5, 11)$

In this section, we will extend $S(4, 5, 11)$ to $S(5, 6, 12)$ by adding one point and show that $S(5, 6, 12)$ exists. We start showing the uniqueness of $S(4, 5, 11)$ up to isomorphism.

Theorem 5.3.1. *There is a unique $S(4, 5, 11)$ Steiner system up to isomorphism.*

Proof. Let S be $S(4, 5, 11)$ and $\alpha, \beta \in S$. If we remove α and β from S we have $S(2, 3, 9)$, which is unique by Theorem 5.1.1. When we add α and β to $S(2, 3, 9)$, quadrangles in the blocks of $S(4, 5, 11)$ are chosen from S_1, S_2 and S_3. We note that each S_i contains 18 blocks by Theorem 5.1.4. Since $Aut(S(2, 3, 9))$ acts transitively on $\{S_1, S_2, S_3\}$ by in the proof of Theorem 5.2.1, where we take 18 blocks does not matter. Therefore $S(4, 5, 11)$ is unique up to isomorphism. □

Now, we will show the one-point extension of $S(4, 5, 11)$ in order to obtain $S(5, 6, 12)$. Our process will be similar to previous section. Then we start assuming that we already have an $S(5, 6, 12)$. Let us pick three points α, β, and γ in $S(5, 6, 12)$. If we remove α from $S(5, 6, 12)$ we have $S(4, 5, 11)$. In the same manner, if we remove β from $S(5, 6, 12)$ we have $S(4, 5, 11)$.

Also if we remove γ from $S(5, 6, 12)$ we have $S(4, 5, 11)$. Since $S(4, 5, 11)$ is unique up to isomorphism by Theorem 5.3.1, the contractions of $S(5, 6, 12)$ due to α, β, and

γ are isomorphic. Then these are one-point extension of $S(3,4,10)$. Also we note that $S(3,4,10)$ is a one-point extension of $S(2,3,9)$. Thus we can say that the set of points of $S(5,6,12)$ consists of points of $S(2,3,9)$, α, β, and γ.

Hence the blocks of $S(5,6,12)$ containing α, β or γ are the following forms:

(i) $\Omega \cup \{\alpha, \beta, \gamma\}$

In this type of block, Ω is a block (line) of $S(2,3,9)$. Since there are 12 such Ω, we have 12 such form of $\Omega \ \cup \ \{\alpha, \beta, \gamma\}$.

(ii) $\Xi \cup \{\beta, \gamma\}$

In this type of block, Ξ is a quadrangle from S_i that is defined in the section 5.1. Since there are 18 such Ξ in S_i, we have 18 such form of $\Xi \cup \{\beta, \gamma\}$. Without loss of generality we pick S_1 for Ξ so as to have $\Xi \cup \{\beta, \gamma\}$.

(iii) $\Xi \cup \{\alpha, \gamma\}$

In this type of block, Ξ is a quadrangle from S_i that is defined in the section 5.1. Since there are 18 such Ξ in S_i, we have 18 such form of $\Xi \cup \{\alpha, \gamma\}$. Without loss of generality we pick S_2 for Ξ so as to have $\Xi \cup \{\alpha, \gamma\}$.

(iv) $\Xi \cup \{\alpha, \beta\}$

In this type of block, Ξ is a quadrangle from S_3 that is defined in the section 5.1. since every set of four points is uniquely involved in blocks. Then there are 18 such Ξ in S_3, and so we have 18 such form of $\Xi \cup \{\alpha, \beta\}$.

For the other blocks we will define a new set of subsets from $S(2,3,9)$. In each S_i, we will call set of $\Xi \cup \{\delta\}$ C_i where $\Xi \in S_i$ and δ is the diagonal point of Ξ.

(*v*) $R \cup \{\alpha\}$

In this type of block, R is a set of quadrangle Ξ from S_i and its diagonal point. Since there are 18 such Ξ in S_i, we have 18 such form of $R \cup \{\alpha\}$. Without loss of generality we pick S_1 for Ξ to have $R \cup \{\alpha\} = C_1$.

(*vi*) $R \cup \{\beta\}$

In this type of block, R is a set of quadrangle Ξ from S_i and its diagonal point. Since there are 18 such Ξ in S_i, we have 18 such form of $R \cup \{\beta\}$. Without loss of generality we pick S_2 for Ξ to have $R \cup \{\beta\} = C_2$.

(*vii*) $R \cup \{\gamma\}$

In this type of block, R is a set of quadrangle Ξ from S_3 and its diagonal point since we have already chosen R from S_1 and S_2. Then there are 18 such Ξ in S_3, and so we have 18 such form of $R \cup \{\gamma\} = C_3$.

Now, we will consider blocks that do not contain α, β or γ. Then blocks that we are looking for can not contain any set of five points in $C_i (i = 1, 2, 3)$.

We will choose six points from $S(2, 3, 9)$ to form a block. By Lemma 5.2.3, we know that any set of five points contains a quadrangle. Hence we should avoid the diagonal point of a quadrangle from a block that we are trying to build. Without loss of generality, we consider a quadrangle with parallel class pair $\{a, b\}$. Then the diagonal point can not lie in four lines of a pair $\{a, b\}$. Therefore, the diagonal point lies in third line of a or third line of b. In other words, The diagonal point is the common point of third line of a and third line of b. If we choose six points from two distinct parallel lines then we will not get diagonal point. Hence, the block of this type is the following:

(*vii*) a union of two distinct parallel lines in $S(2, 3, 9)$.

To sum up, we have shown 132 blocks in total. Therefore $S(5, 6, 12)$ exists.

Theorem 5.3.2. *There is a unique* $S(5, 6, 12)$ *Steiner system up to isomorphism.*

Proof. The strategy is similar to the proof of Theorem 5.3.1 since the uniqueness of $S(5, 6, 12)$ is also depended on quadrangles of $S(2, 3, 9)$. The points of $S(5, 6, 12)$ consists of points of $S(2, 3, 9)$ and three further points. We find out the blocks of $S(5, 6, 12)$ in our above discussion and points of blocks based on the points of $S(2, 3, 9)$. Since $Aut(S(2, 3, 9))$ acts transitively on points of $S(2, 3, 9)$, $S(5, 6, 12)$ is unique. □

Chapter 6

The binary Golay code and $S(5, 8, 24)$

In this chapter, we will form $S(5, 8, 24)$ and the binary Golay code simultaneously and conclude that they are the same structure. We will follow Robin J. Chapman's article [20] and P. J. Cameron and J. H. van Lint's book [21]. We note that R. J. Chapman's article is actually recollection of John H. Conway's lectures that can be found in [22].

6.1 Coding theory

In this section, we will introduce coding theory briefly. We consider a set $\mathbf{F}$ as a collection of q distinct symbols that is called an *alphabet*. In general, one may take $q = p^r$ where p is a prime and $\mathbf{F} = \mathbf{F}_q$. Then the code is called a *q-ary* code. If $q = 2$ we call it *binary* code. Also we regard $\mathbf{F}$ as 1-dimensional vector space over the field $\mathbf{F}$.

Definition 6.1.1. We may form n-tuples by using the symbols of $\mathbf{F}$. We call these n-tuples *words* and n the *word length*. We denote the set of all words of length n by $\mathbf{F}^n$. We regard it as n-dimensional vector space over the field $\mathbf{F}$.

Definition 6.1.2. Let $x \in \mathbf{F}^n$ and $y \in \mathbf{F}^n$. The distance function d is defined as the number of coordinate places in which x and y differ and is denoted by $d(x, y)$. That is to say,

$$d(x, y) = |\{i : 1 \leq i \leq n;\ x_i \neq y_i\}|.$$

The distance function d is called the *Hamming distance*. As in our definition, it measures difference of the positions in two n-tuples. If $d(x, y) = 0$ then we have $x = y$. Also $d(x, y) = d(y, x)$, and so d is symmetric. Let $z \in \mathbf{F}^n$. Then $d(x, y) + d(y, z) \geq d(x, z)$ since if there is a difference in the ith coordinate between x and z then there should be a difference in the ith coordinate between x and y or y and z. Therefore d is the metric.

For the next definition, we consider y as 0, that is the zero vector in $\mathbf{F}^n$.

Definition 6.1.3. The *weight* of $x \in \mathbf{F}^n$ is $w(x) := d(x, 0)$. That is, $w(x)$ is the number of non-zero entries in x.

Definition 6.1.4. The *ball* of radius ρ with centre at $x \in \mathbf{F}^n$ where $\rho > 0$ is

$$B(x, \rho) := \{y \in \mathbf{F}^n : d(x, y) \leq \rho\}.$$

Now, we will form a special subset $\mathcal{C}$ of $\mathbf{F}^n$. The property of $\mathcal{C}$ is that any two distinct words of $\mathcal{C}$ have distance at least $2e + 1$. Let us pick any x in $\mathcal{C}$. Then we change t coordinates of x where $t \leq e$ to yield a new word x'. Since the distance between x and x' is t and $t < 2e + 1$, x' looks like x more than any other words of $\mathcal{C}$. As a result, we can correct the t errors if we know $\mathcal{C}$. A subset $\mathcal{C}$ is called *e-error-correcting* code. Formal definition as follows.

Definition 6.1.5. An *e-error-correcting* code $\mathcal{C}$ is a subset of $\mathbf{F}^n$ with the property

$$\forall_{x\in\mathcal{C}}\forall_{y\in\mathcal{C}}[x \neq y \Rightarrow d(x,y) \geq 2e+1].$$

Remark 6.1.6. We may call words in $\mathcal{C}$ *codewords*.

We interpret that balls of radius e of two distinct codewords are disjoint in $\mathcal{C}$. If balls in $\mathcal{C}$ cover $\mathbf{F}^n$ then the code is called $perfect$. Formal definition as follows.

Definition 6.1.7. An *e-error-correcting* code $\mathcal{C}$ in $\mathbf{F}^n$ is called $perfect$ if

$$\bigcup_{x\in\mathcal{C}} B(x,e) = \mathbf{F}^n.$$

Definition 6.1.8. A k-dimensional linear subspace $\mathcal{C}$ of $\mathbf{F}^n$ is called a *linear code* over the field F.

Proposition 6.1.9. *The minimum distance of a linear code $\mathcal{C}$ is the minimum weight of a codeword in $\mathcal{C}$.*

Proof. Let x and y be in $\mathcal{C}$. Since $\mathcal{C}$ is linear subspace, $x-y$ is in $\mathcal{C}$. Then we have $d(x,y) = d(x-y,0) = w(x-y)$. □

Definition 6.1.10. Let $\mathcal{C}$ be a k-dimensional linear code. Then

$$\mathcal{C}^\perp := \{x \in \mathbf{F}^n : \forall_{y\in C}[\langle x,y\rangle = 0]\},$$

where $\langle x,y\rangle$ denotes the dot product in $\mathbf{F}^n$, is called the *dual code* of $\mathcal{C}$ of $(n-k)$-dimensional linear code. That is; $dim\ \mathcal{C} + dim\ \mathcal{C}^\perp = n$.

Definition 6.1.11. A code $\mathcal{C}$ is called $self$-*dual* and $dim\ \mathcal{C} = n/2$ if $\mathcal{C} = \mathcal{C}^\perp$. If $\mathcal{C} \subseteq \mathcal{C}^\perp$ then $\mathcal{C}$ is called $self$-*orthogonal* and $dim\ \mathcal{C} \leq n/2$.

Definition 6.1.12. Let $\mathcal{C}$ be a code of length n and let A_i denote the number of codewords of weight i where $i = 0, 1, ..., n$. Then

$$A(x) := \sum_{i=0}^{n} A_i x^i$$

is called the *weight enumerator* of $\mathcal{C}$.

We have made our definitions in a general setting. Now, let consider binary linear code of length n, say $\mathcal{C}$, in more detail. As we had mentioned earlier, if $q = 2$ and $\mathcal{C}$ is a linear subspace of $\mathbf{F}_2^n$ then $\mathcal{C}$ is called *binary linear code*.

We will define codewords of $\mathcal{C}$ in terms of subsets of $\{1, 2, ..., n\}$. Let a be in $\mathcal{C}$. Since a is an n-tuple, we can write a explicitly as $a = (a_1\ a_2\ ...\ a_n)$ or $a = (a_j)$ where $j \in \{1, 2, ..., n\}$. Then we identify a with where a_j is 1. Hence we form a set, say A, of all j with $a_j = 1$. A is a subset of $\{1, 2, ..., n\}$ and we define a as the subset A. With this new definition, $\mathbf{F}_2^n$ becomes the power set of $\{1, 2, ..., n\}$.

Now, we make some definitions regarding the binary linear code $\mathcal{C}$.

Let $\mathcal{X}$ be a set $\{1, 2, ..., n\}$ and $\mathcal{C}$ be a binary linear code of the power set of $\mathcal{X}$, namely $\mathcal{P}(\mathcal{X})$. For all A, B in $\mathcal{P}(\mathcal{X})$, addition is defined by symmetric difference, namely $A + B := (A \cup B) - (A \cap B)$, and multiplication is defined by $AB := |A \cap B|$ in *mod* 2.

Definition 6.1.13. The *length* of $\mathcal{C}$ is the order of $\mathcal{X}$, namely $|\mathcal{X}|$.

Definition 6.1.14. Let A, B be in $\mathcal{P}(\mathcal{X})$. Then the *weight* $w(A)$ of A is the order of A, namely $|A|$. Also the *weight* $w(A + B)$ of $A + B$ is the order of $A + B$, namely $|A + B|$.

Since $|A+B| = |A|+|B|-2|A\cap B|$, $w(A+B) \equiv w(A)+w(B)$ in *mod* 2. Moreover if $AB = 0$ then $|A \cap B|$ is even, and so $w(A + B) \equiv w(A) + w(B)$ in *mod* 4.

Definition 6.1.15. We call $\mathcal{C}$ *even* if the order of every non-empty subset of $\mathcal{C}$ is even and also call $\mathcal{C}$ *doubly even* if the order of every non-empty subset of $\mathcal{C}$ is divisible by 4.

Definition 6.1.16. Let $\mathcal{C}$ be a code of $\mathcal{P}(\mathcal{X})$. Then

$$C^{\perp} = \{A \in \mathcal{P}(\mathcal{X}) : \forall_{B \in C}[AB = |A \cap B| \equiv 0\ mod\ 2]\}$$

is the *dual* of $\mathcal{C}$.

Proposition 6.1.17. *Let $\mathcal{C}$ be a self-orthogonal and $\mathcal{H}$ be a subset of $\mathcal{C}$ of words of weights divisible by 4. If $\mathcal{C}$ is spanned by $\mathcal{H}$ then $\mathcal{C}$ is called doubly even. Conversely, if $\mathcal{C}$ is doubly even then C is self-orthogonal.*

Proof. We suppose that $\mathcal{C}$ is spanned by $\mathcal{H}$, where $\mathcal{H} = \{A \in \mathcal{C} : w(A) \equiv 0 \ mod\ 4\}$. Let $B \in \mathcal{C}$. Then B can be represented by the summation of some elements of $\mathcal{H}$. Also since $\mathcal{C}$ is self-orthogonal, $w(B) \equiv 0 \ mod\ 4$. Therefore $\mathcal{C}$ is doubly even by Definition 6.1.15.

Conversely, we suppose that $\mathcal{C}$ is doubly even. Let $A, B \in \mathcal{C}$. Since $A + B \in C$, its order is divisible by 4. This means that $|A \cap B|$ is even. Hence $AB = 0$. Therefore $C \subseteq C^{\perp}$ and so C is self-orthogonal by Definition 6.1.11. □

Definition 6.1.18. The *minimum weight* of $\mathcal{C}$ is the order of the smallest non-zero subset in C.

Definition 6.1.19. Let $\mathcal{C}$ be at least 12-dimensional. If every codewords' length is 24 and the minimum weight of $\mathcal{C}$ is at least 8 then we call $\mathcal{C}$ *binary Golay code*.

6.2 Construction

Theorem 6.2.1. *Let $\mathcal{X}$ be a set of order 24 and $\mathcal{C}$ be a subspace of $\mathcal{P}(\mathcal{X}) = V$. If $\mathcal{C}$ is a binary Golay code then it is exactly 12-dimensional.*

Proof. Let x be fixed in $\mathcal{X}$. Then we want to count such sets in V with the order less than or equal to 4 or containing x have the order 4. We have 24 elements in $\mathcal{X}$. It follows that $\binom{24}{1}$ is the number of sets of one element. Similarly, $\binom{24}{2}$ is the number of sets of two elements and $\binom{24}{3}$ is the number of sets of three elements. If we count

x in the sets then the number of sets of four elements is $\binom{23}{3}$. Also there is an empty set. In short, the total number of sets we would like to count is as follows,

$$\binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \binom{23}{3} = 4096 = 2^{12}.$$

We call this family of sets $\mathcal{M}$. Let $A, B \in \mathcal{M}$. We suppose that the orders of A and B are 4. Thus $x \in A \cap B$. For this reason, the weight of $A + B$ can be at most 6. Similarly, if the orders of A and B are less than 4 then the weight of $A + B$ can be at most 6. Hence $A + B \notin \mathcal{C}$ since the weight must be at least 8 by Definition 6.1.19. Since the cosets $A + \mathcal{C}$ are all distinct, the order of set of cosets is at least 2^{12}. Also we note that $|\mathcal{C}| \geq 2^{12}$. Then it follows that the order of set of cosets must be at most 2^{12}. Therefore $|\mathcal{C}| = 2^{12}$, and so $\mathcal{C}$ is exactly 12-dimensional. □

Theorem 6.2.2. *Let $\mathcal{X}$ be a set of order 24 and $\mathcal{C}$ be a subspace of $\mathcal{P}(\mathcal{X}) = V$. If $\mathcal{C}$ is a binary Golay code then*

(*i*) *the weight of the smallest non-zero subset of $\mathcal{C}$ is 8.*

(*ii*) *the words of weight 8 in $\mathcal{C}$ form $S(5, 8, 24)$.*

Proof. (*i*) Let B in V but not in $\mathcal{M}$ and $|B| = 4$. Then $B \in A + \mathcal{C}$ for some $A \in \mathcal{M}$. Hence $A + B \in \mathcal{C}$. This implies that $|A| = 4$ and $|A + B| = 8$. Therefore the minimum weight of $\mathcal{C}$ is 8.

(*ii*) We continue with the result of the first part. We have shown that $|A + B| = 8$. Since $|A| = 4$ and $A \in \mathcal{M}$, we have $x \in A$. It follows that $|\{x\} \cup B| = 5$ and $\{x\} \cup B \subset A + B$. This means that sets of five elements containing x are contained in at least one set of eight elements of $\mathcal{C}$. Since x was chosen arbitrarily, we can generalize the last sentence as follows. Any sets of five elements are contained in at least one set of eight elements of $\mathcal{C}$.

Now we suppose that there exist distinct sets of $\mathcal{C}$, say N, M, such that they have weight 8 and also contain the same set of five elements, say L. That is to say, $L \subseteq N \cap M$. It follows that the weight of $N + M$ is at most 6. Since $N + M \in \mathcal{C}$, we get a contradiction. Therefore $N = M$ and any sets of five elements are contained in exactly one set of eight elements of $\mathcal{C}$.

In conclusion, the words of weight 8 form $S(5, 8, 24)$ by Definition 3.1.1. □

Theorem 6.2.3. *Let $\mathcal{X}$ be a set of order 24 and $\mathcal{C}$ be a subspace of $\mathcal{P}(\mathcal{X}) = V$. If $\mathcal{C}$ is a binary Golay code then it is spanned by the words of weight 8.*

Proof. Let $\mathcal{C}' \subseteq \mathcal{C}$ such that it is generated by the set of words of weight 8. We want to show that $\mathcal{C}' \supseteq \mathcal{C}$. Let A be in V such that $|A| \geq 5$. Then by Theorem 6.2.2, there exists a set B of weight 8 in $\mathcal{C}$ such that $|A \cap B| \geq 5$. This implies that $|A + B| < |A|$, and so $|A + B| \leq 4$. Also by Theorem 6.2.2, we know that if B in V but not in $\mathcal{M}$ and $|B| = 4$ then there exists $A \in \mathcal{M}$ such that $A + B \in \mathcal{C}$ and $|A + B| = 8$. Hence we can say that every element of V is congruent to elements of $\mathcal{M}$ in *modulo* $\mathcal{C}'$. Therefore $\mathcal{C}' \supseteq \mathcal{C}$, and so $\mathcal{C}' = \mathcal{C}$ □

Theorem 6.2.4. *Let $\mathcal{X}$ be a set of order 24 and $\mathcal{C}$ be a subspace of $\mathcal{P}(\mathcal{X}) = V$. Also let $S = S(5, 8, 24)$ on $\mathcal{X}$. Suppose that $\mathcal{C}$ is spanned by the blocks A in S. Then*

(i) $\mathcal{C}$ is self-dual.

(ii) $\mathcal{C}$ is a binary Golay code and its weight enumerator is

$$1 + 759x^8 + 2576x^{12} + 759x^{16} + 1x^{24}.$$

(iii) The words of weight 8 are blocks of S.

Proof. (i) We know that if $\mathcal{C} = \mathcal{C}^{\perp}$ then $\mathcal{C}$ is self-dual from Definition 6.1.11. For this purpose we will firstly show that for all $A, B \in S$, we have $|A \cap B|$ is even.

Let us fix $A \in S$ and let I be a subset of A. We calculate the number of elements of S containing I by using the intersection triangle of S. Let $|I| = i$. Then the coordinates of the intersection triangle as follows from Definition 3.2.4.

$$\lambda_{i,0} = \begin{cases} \frac{\binom{24-i}{5-i}}{\binom{8-i}{5-i}} \text{ when } & 0 \leq i \leq 5 \\ 1 \quad \text{when} & 5 < i \leq 8 \ , \end{cases}$$

We compute $\lambda_{0,0} = 759$, $\lambda_{1,0} = 253$, $\lambda_{2,0} = 77$, $\lambda_{3,0} = 21$, $\lambda_{4,0} = 5$, $\lambda_{5,0} = \lambda_{6,0} = \lambda_{7,0} = \lambda_{8,0} = 1$.

Let C, D be subsets of A such that $C \subseteq D$. Also let $|C| = i$ and $|D| = j$. If $B \in S$ then we want to compute the number of B in S such that $B \cap D = C$. Then if $i = j$ then the number of B is $\lambda_{i,0}$. Now we suppose that $i < j$. Then there exists $C^{'}$ such that $C \cup C^{'} = D$ and $|C^{'}| = j - i$.

That is to say, we are looking for blocks containing C but not containing all elements of $C^{'}$. Hence the number of blocks of this kind is the relation as in the Definition 3.2.4, namely $\lambda_{i,j-i} = \lambda_{i,j-i-1} - \lambda_{i+1,j-i-1}$ for $j - i \geq 1$. Also if $j = 8$ then $D \in S$. It follows that $\lambda_{i,8-i}$ is 0 for all odd i. Therefore the intersection of each two elements of S has even order. This means that $\mathcal{C}$ is spanned by mutually orthogonal sets in $\mathcal{P}(\mathcal{X})$. Thus $\mathcal{C}$ is self-orthogonal, and so $dim\ \mathcal{C} \leq n/2$. Also from the proof of the Theorem 6.2.1, we have $dim\ \mathcal{C} \geq n/2$. Therefore $dim\ \mathcal{C} = n/2$ and so $\mathcal{C} = \mathcal{C}^{\perp}$ by Definition 6.1.11.

(ii) We suppose that $\mathcal{C}$ is spanned by A in S. Then since $|A|$ is divisible by 4, $\mathcal{C}$ is doubly even by Definition 6.1.15. Let A_i denote the number of codewords of weight i where $i = 0, 1, ..., 24$. Since $\mathcal{C}$ is doubly even, $A_i = 0$ for all i not divisible by 4. Thus the weight enumerator of $\mathcal{C}$ is as follows by Definition 6.1.12.

$$A(x) = A_0x^0 + A_4x^4 + A_8x^8 + A_{12}x^{12} + A_{16}x^{16} + A_{20}x^{20} + A_{24}x^{24}.$$

We note that the minimum weight of $\mathcal{C}$ is at least 8. For this reason, if we show that

$A_4 = 0$ then $\mathcal{C}$ will be a binary Golay code. Then let $A \in \mathcal{C}$ such that $|A| = 4$. If $A \in \mathcal{M}$ defined in the proof of Theorem 6.2.1 then $A + \mathcal{C}$ form a coset of $\mathcal{C}$. Since $|\mathcal{M}| = 2^{12}$, distinct elements of $\mathcal{M}$ are not congruent to each other modulo $\mathcal{C}$. If $A \in \mathcal{C}$ then we may have $A = B + C$ for some distinct elements B, C in $\mathcal{M}$ such that $|B| = 2, |C| = 2$. But B and C are congruent to each other. Hence we get a contradiction. Therefore there is no set of weight 4 in $\mathcal{C}$ and so $\mathcal{C}$ is a binary Golay code.

We can easily see that $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$ and $A_{12} = 2576$. Therefore the weight enumerator of $\mathcal{C}$ is

$$A(x) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + 1x^{24}.$$

(*iii*) It is the immediate result of Theorem 6.2.2. □

We see that construction of a binary Golay code is same as construction of $S(5, 8, 24)$.

Chapter 7

Simplicity of the Mathieu Groups

In this chapter we will show the simplicity of the Mathieu groups. The entire chapter will be based on Robin J. Chapman's article [14] and Simon Rubinstein-Salzedo's article [15].

7.1 Preliminaries

Let S_p be a symmetric group of degree p in which p is a prime number. Also let G be a subgroup of S_p. Then G acts on a set of p elements, namely $\{1, 2, ..., p\}$.

Lemma 7.1.1. *G acts transitively on $\{1, 2, ..., p\}$ if and only if $p \mid |G|$ and a cyclic Sylow p-subgroup exists in G.*

Proof. Let $X = \{1, 2, ..., p\}$ and $x \in X$. Then we suppose that G acts transitively on X. This means that X has just one orbit. Thus by the Orbit-Stabiliser Theorem (2.1.18), we have $|X| = |G : G_x|$. Hence $p \mid |G|$.

We note that $|S_p| = p!$. Also since G is a subgroup of S_p, we have $|G| \mid |S_p|$, and so $|G| = pm$ where $p \nmid m$. As a result, G has a Sylow p-subgroup of order p by Sylow's Existence Theorem (2.1.33). Since groups of prime order are cyclic, a cyclic Sylow p-subgroup exists in G.

For the converse, we suppose that $p \mid |G|$ and a cyclic Sylow p-subgroup, say P, exists in G. Then let $P = \langle \pi \rangle$ where $\pi = (1\ 2 ...\ p)$. It follows that for any $x, y \in X$ there exists π^i for some $1 \leq i \leq p$ such that $\pi^i x = y$. Therefore G acts transitively on X. □

Lemma 7.1.2. *Let G be a group of order n and P be a cyclic Sylow p-subgroup of G. Also let n_G be the number of Sylow p-subgroups of G and $r_G = |N_G(P) : P|$. Then $|G| = pr_G n_G$.*

Proof. From Sylow's Theorem (2.1.34), we know that $n_G = |G : N_G(P)|$. So we can decompose order n of the group G as follows:

$$n = |G| = |G : N_G(P)||N_G(P) : P||P| = pr_G n_G.$$

□

Lemma 7.1.3. *Let $r_G = |N_G(P) : P|$. Then r_G is congruent to $\frac{n}{p}$ in mod p.*

Proof. By Sylow's Theorem (2.1.34), we have $n_G \equiv 1\ (mod\ p)$. We suppose that $P = \langle (1\ 2 ...\ p) \rangle$ and $\pi = (1\ 2 ...\ p)$. Let $\sigma \in N_{S_p}(P)$. Then $\sigma P \sigma^{-1} = P$ and so $\sigma\pi\sigma^{-1} = \pi^k$. For $k = 1$, we have $\sigma\pi\sigma^{-1} = \pi = (\sigma(1)\ \sigma(2) ...\ \sigma(p))$. Hence, we have p different σ satisfying $\sigma\pi\sigma^{-1} = \pi$. Thus $C_{S_p}(P) = P$. Since we can choose k up to $p - 1$, we get $|N_{S_p}(P)| = p(p - 1)$.

It follows that r_G is a factor of $p - 1$; hence $1 \leq r_G \leq p - 1$. Since $\frac{n}{p} = r_G n_G$ and $n_G \equiv 1\ (mod\ p)$ by Lemma 7.1.2, this implies that $r_G \equiv \frac{n}{p}\ (mod\ p)$. □

Lemma 7.1.4. *Let $G \leq S_p$ act transitively on $X = \{1, 2, ..., p\}$. Also let $r_G = |N_G(P) : P|$ and $n_G = |G : N_G(P)|$. If $n_G > 1$ then $r_G > 1$.*

Proof. Let $|G| = n$. We suppose that $n_G > 1$ and $r_G = 1$. Thus $|G| = n = pn_G$ by Lemma 7.1.2. Since a cyclic group of order p has $p - 1$ generators and n_G is the number of distinct cyclic groups of order p, the number of elements of order p is $n_G(p - 1) = n - n_G$. Moreover, these elements permute all points in X since their order is p. Hence there are at most n_G elements that permute not all points of X.

We note that G acts transitively on X. Thus $|\mathcal{O}(x)| = p$ for all $x \in X$. Then by the Orbit-Stabiliser Theorem (2.1.18), we have $|\mathcal{O}(x)||G_x| = |G|$. Hence $|G_x| = n/p = n_G$ for all $x \in X$. This means that stabilisers of every x in X are the same. Since the identity element is the only element fixing every x in X, we have $n_G = 1$. Therefore, we get a contradiction. □

Corollary 7.1.4.1. *Let $G \leq S_p$ act transitively on $X = \{1, 2, ..., p\}$ and $r_G = 1$. Then $G \cong \mathbb{Z}_p$.*

Proof. Let $r_G = 1$ and $|G| = n$. From previous lemma's proof, we know that G has $n - n_G$ elements of order p and $|G_x| = n_G = 1$ for all $x \in X$. Since $|G| = n = pr_G n_G$ by Lemma 7.1.2, we have $|G| = p$. Therefore $G \cong \mathbb{Z}_p$. □

Theorem 7.1.5. *Let $G \leq S_p$ act transitively on $X = \{1, 2, ..., p\}$. Also let $|G| = pmr$ such that $m > 1$ and $m \equiv 1 \pmod p$, $r < p$ and r is prime. Then G is simple.*

Proof. Let $r = r_G$ and $m = n_G$ where r_G and n_G defined as in Lemma 7.1.2. Also let $H \lhd G$ be non-trivial. Then H acts on X. It follows that Hx is block for any $x \in X$ by Theorem 2.1.52 and Hx is also an orbit of the action of H on X. Since G acts transitively and H is non-trivial subgroup, $|Hx| = s > 1$ for all $x \in X$. As a result, $|Hx| = s = p$. Thus H acts transitively on X.

There is a Sylow p-subgroup of G, say P', such that $P' \leq H$ by Lemma 7.1.1. Since any two Sylow p-subgroups of G are conjugate in G, all Sylow p-subgroups of G are contained in H. This means that the number of Sylow p-subgroups of H is equal to the number of Sylow p-subgroups of G, namely $n_G = n_H$. Also we have $|H| = pn_H t = pn_G t$. Then $t \mid r$ by Lagrange's Theorem (2.1.30). Also $t > 1$ by Lemma 7.1.4. Since r is a prime number, we have $t = r$. Hence $|H| = |G|$ and so $H = G$. Therefore G is simple. □

Now, we will show some theorems that we give without proofs. We follow chapter 9 of the book [8] of J. J. Rotman for pages between 286-292. We will use these theorems in section 7.2. More specifically, we will use Theorem 7.1.6 and Theorem 7.1.7 to show the simplicity of M_{11} and M_{23}. Also we study multiply transitive groups in section 2.1.4 in chapter 2 and develop simplicity criterion Theorem 2.1.59. Then we will use it with Theorem 7.1.8, Theorem 7.1.9 and Theorem 7.1.10 to show the simplicity of the remaining Mathieu groups.

Theorem 7.1.6. [8, Theorem 9.52, page 288] *The order of the Mathieu Group M_{11} is* 7920.

Theorem 7.1.7. [8, Theorem 9.56, page 291] *The order of the Mathieu Group M_{23} is* 10200960.

Theorem 7.1.8. [8, Theorem 9.53, page 289] *M_{12} is a* 5*-transitive group such that the stabiliser of a point in M_{12} is M_{11}.*

Theorem 7.1.9. [8, Theorem 9.55, page 290] *M_{22} is a* 3*-transitive group such that the stabiliser of a point in M_{22} is $PSL_3(\mathbb{F}_4)$.*

Theorem 7.1.10. [8, Theorem 9.57, page 292] *M_{24} is a* 5*-transitive group such that the stabiliser of a point in M_{24} is M_{23}.*

7.2 Results

Theorem 7.2.1. *The Mathieu Groups M_{11} and M_{23} are simple.*

Proof. Now, $M_{11} < S_{11}$, and $|M_{11}| = 7920$ by Theorem 7.1.6. By Lemma 7.1.3, $r_{M_{11}} \equiv \frac{n}{p} = \frac{|M_{11}|}{11} = 720 \equiv 5 \ (mod\ 11)$. This implies that $r_{M_{11}} = 5$ and $m_{M_{11}} = 144 > 1$. Thus, $m_{M_{11}} \equiv 1 \ (mod\ 11)$, $r_{M_{11}} < 11$ and $r_{M_{11}}$ is prime. Therefore, by Theorem 7.1.5, M_{11} is simple.

Also, $M_{23} < S_{23}$, and $|M_{23}| = 10200960$ by Theorem 7.1.7. By Lemma 7.1.3, $r_{M_{23}} \equiv \frac{n}{p} = \frac{|M_{23}|}{23} = 443520 \equiv 11 \ (mod\ 23)$. This implies that $r_{M_{23}} = 11$ and $m_{M_{23}} = 40320 > 1$. Thus, $m_{M_{23}} \equiv 1 \ (mod\ 23)$, $r_{M_{23}} < 23$ and $r_{M_{23}}$ is prime. Therefore, by Theorem 7.1.5, M_{23} is simple. □

Also, we want to show that the Mathieu groups M_{12},M_{24} and M_{22} are simple too.

Theorem 7.2.2. *The Mathieu Groups M_{12},M_{24} and M_{22} are simple.*

Proof. M_{12} is 5-transitive group whose stabiliser at any point is M_{11} by Theorem 7.1.8. Then M_{11} is a simple group by Theorem 7.2.1. Therefore M_{12} is simple by Theorem 2.1.59.

M_{24} is 5-transitive group whose stabiliser at any point is M_{23} by Theorem 7.1.10. Then M_{23} is a simple group by Theorem 7.2.1. Therefore M_{24} is simple by Theorem 2.1.59.

M_{22} is 3-transitive group whose stabiliser at any point is $PSL_3(\mathbb{F}_4)$ by Theorem 7.1.9. Then $PSL_3(\mathbb{F}_4)$ is a simple group [8, Theorem 8.23, page 232]. Therefore M_{22} is simple by Theorem 2.1.59. □

Bibliography

[1] E. Mathieu, "Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables.," *Journal de Mathématiques Pures et Appliquées*, pp. 241–323, 1861.

[2] E. Mathieu, "Sur la fonction cinq fois transitive de 24 quantités.," *Journal de Mathématiques Pures et Appliquées*, pp. 25–46, 1873.

[3] M. Aschbacher, "The status of the classification of the finite simple groups," *Notices Amer. Math. Soc.*, vol. 51, no. 7, pp. 736–740, 2004.

[4] R. Solomon, "A brief history of the classification of the finite simple groups," *Bull. Amer. Math. Soc. (N.S.)*, vol. 38, no. 3, pp. 315–352, 2001.

[5] E. Witt, "über Steinersche Systeme," *Abh. Math. Sem. Univ. Hamburg*, vol. 12, no. 1, pp. 265–275, 1937.

[6] D. S. Malik, J. N. Mordeson, and M. K. Sen, *Fundamentals of Abstract Algebra*. International series in pure and applied mathematics, McGraw-Hill Book Company, Inc., New York, 1997.

[7] J. J. Rotman, *A first course in abstract algebra: with application*. Prentice Hall, Inc., Upper Saddle River, NJ, third ed., 2006.

[8] J. J. Rotman, *An introduction to the theory of groups*, vol. 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth ed., 1995.

[9] D. S. Dummit and R. M. Foote, *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third ed., 2004.

[10] I. M. Isaacs, *Finite group theory*, vol. 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[11] N. L. Biggs and A. T. White, *Permutation groups and combinatorial structures*, vol. 33 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge-New York, 1979.

[12] G. E. Moorhouse, "Incidence geometry." 2017.

[13] B. De Bruyn, *An introduction to incidence geometry*. Frontiers in Mathematics, Birkhäuser/Springer, Cham, 2016.

[14] R. J. Chapman, "An elementary proof of the simplicity of the Mathieu groups M_{11} and M_{23}," *Amer. Math. Monthly*, vol. 102, no. 6, pp. 544–545, 1995.

[15] S. Rubinstein-Salzedo, "Mathieu groups." 2011.

[16] J. D. Dixon and B. Mortimer, *Permutation groups*, vol. 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[17] C. J. Colbourn and J. H. Dinitz, eds., *Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, second ed., 2007.

[18] P. J. Cameron, *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, Cambridge, 1994.

[19] H. Havlicek and H. Lenz, "Another simple proof for the existence of the small Witt design," *Elem. Math.*, vol. 56, no. 3, pp. 89–94, 2001.

[20] R. J. Chapman, "Constructions of the golay codes: A survey." 1997.

[21] P. J. Cameron and J. H. van Lint, *Designs, graphs, codes and their links*, vol. 22 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[22] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, vol. 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third ed., 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.