

# Diameters of orbital graphs associated to groups

Tom Smith

Supervised by Dr Benjamin Klopsch

Technical Report

RHUL-MA-2009-23

28 October 2009



Department of Mathematics  
Royal Holloway, University of London  
Egham, Surrey TW20 0EX, England

<http://www.rhul.ac.uk/mathematics/techreports>

## Abstract

Associated to groups are a number of graphs, in particular the diameters of orbital graphs associated to primitive groups are of interest. Some work has been performed to describe infinite families of finite primitive permutation groups with a uniform finite upper bound on their orbital graphs. However explicit bounds for smaller families of groups remain a rich area of mathematical research. This paper aims to first build the foundations of group theory before discussing the orbital graphs of primitive groups, before engaging in the direct computation of the diameters of orbital graphs associated to projective special linear groups  $\text{PSL}(2, p)$  for primes  $p < 200$ . Based on the evidence gathered from these computations, we formulate several concrete conjectures.

## Acknowledgements

This research project was funded by the Nuffield Foundation as part of their science bursaries 2009 scheme for undergraduate research, their generous grant gave me the opportunity to research an area of mathematics over the course of the summer vacation. For this they have my sincerest thanks.

I would also like to thank Dr Benjamin Klopsch of the Royal Holloway mathematics department, without his support and guidance this project would have been unfeasible.

# Contents

1	Introduction	4
2	Basic group theory	6
3	Group Actions	9
4	Primitivity	14
5	Graphs	18
6	Suborbits, orbitals and orbital graphs	20
7	The O’Nan-Scott Theorem	24
8	The Projective Special Linear Groups	29
9	Computations using Magma	31
10	Conclusion	41

# 1 Introduction

The aim of this document is to quickly build the basic ideas behind group theory, before moving to the more specific area of orbital graphs. This work is motivated by a recent paper by M.W. Liebeck, D. Macpherson and K. Tent titled 'Primitive permutation groups of bounded orbital diameter' [1]. In this paper infinite families of finite primitive permutation groups with a uniform finite upper bound on their orbital graphs are described. However these bounds are not explicit, it is the aim of this project to investigate explicit bounds for specific cases. Our main contribution is the direct computation of the diameters of orbital graphs associated to projective special linear groups  $\text{PSL}(2, p)$  for primes  $p < 200$ . Based on the evidence gathered from these computations, we formulate several concrete conjectures. The data collected and the conjectures are stated in Section 9.

Much of the background for this project was obtained from M. Bhattacharjee, D Macpherson, R. G. Möller and P.M Neumann's book titled *Notes on infinite permutation groups* [2], J.D. Dixon and B. Mortimer's book titled simply *Permutation Groups* [3] and the paper *On the O'Nan-Scott theorem for finite primitive permutation groups* by M.W. Liebeck, C.E. Praeger and J. Saxl [4].

Firstly we ask the most important question, the answer to which will provide the scene in which this project is based; what is a group? Groups are essentially an abstract step above (or equally, behind) many of the well known structures in mathematics. Rings, fields and vector spaces are all groups at their heart, furnished with further operations and axioms.

**Definition 1.1** *A group  $G$  consists of a set of elements together with a binary operation;  $\cdot$ , which is a map  $G \times G \rightarrow G$ .*

The set and operation must satisfy three important axioms in order to be a group, namely,

- **Associativity:** Given  $f, g, h \in G$ ,  $(f \cdot g) \cdot h = f \cdot (g \cdot h)$
- **Identity:** There exists an identity element (written as 1 or  $e$ ) in  $G$  such that for all  $g \in G$ ,  $g \cdot e = e \cdot g = g$

- Invertibility: For every  $g \in G$  there is an inverse element written  $g^{-1} \in G$  such that  $g \cdot g^{-1} = g^{-1} \cdot g = e$

Often the operator  $\cdot$  will be omitted and we write  $gh$  instead of  $g \cdot h$ .

Secondly, what is a permutation? Given a set  $\Omega$  of arbitrary elements called points (usually denoted by lowercase greek letters), a permutation on  $\Omega$  is simply a bijection  $\Omega \rightarrow \Omega$ . Clearly if  $|\Omega| = n$  then there are  $n!$  permutations. Together these permutations form a group, with the group operation being functional composition;  $(g \cdot h)(\alpha) = g(h(\alpha))$ , for  $g, h \in G$  and  $\alpha \in \Omega$ .

**Definition 1.2** *The complete collection of permutations on a set  $\Omega$  forms the **symmetric group** denoted  $\text{Sym}(\Omega)$ .*

**Definition 1.3** *A **subgroup**  $H$  of a group  $G$  is a set contained in  $G$  which forms a group under the same operation. It may or may not be equal to  $G$ , if it is not equal we say  $H$  is a **proper subgroup** and write  $H < G$ , else  $H \leq G$ . Clearly  $\{e\}$  is a subgroup, and is known as the *trivial subgroup*.*

A permutation group is any subgroup of a symmetric group. Cayley's theorem (discussed in detail later) shows that every group behaves like a permutation group. This makes permutation groups a very valuable area of study, as what is true for permutation groups is true for groups in general.

## 2 Basic group theory

There are a number of fundamental structures concerning group theory, and this section aims to quickly provide definitions and simple results that will provide a framework and tools instrumental for discussing the area of group theory in which this project lies. These definitions and theorems were largely taken from [2].

**Definition 2.1** *A proper subgroup  $H < G$  is said to be **maximal** if there is no subgroup properly containing  $H$  and properly contained in  $G$ . That is, if  $H$  is maximal any subgroup containing  $H$  must either be equal to  $H$  or equal to  $G$ .*

The concept of maximality is mirrored with the definition of minimality.

**Definition 2.2** *A non-trivial subgroup  $H \leq G$  is said to be **minimal** if  $J \leq H$  implies either  $J = H$  or  $J$  is the trivial group.*

**Definition 2.3** *Given  $H \leq G$  and  $g \in G$ , the **right coset**  $Hg$  is the set  $Hg = \{hg : h \in H\}$ . The **left coset** has the obvious definition.*

It is important to note that when describing a coset, for example  $Hg$ ,  $g$  is known as the *representative* of the coset, the choice of representative is not unique and so we must be careful when dealing with operations involving cosets that the operation is *well defined* and does not depend on our choice of representative. Cosets partition the group, meaning that either  $Ha \cap Hb = \emptyset$  or  $Ha = Hb$ . Since groups are not in general commutative, the left and right cosets of a particular subgroup do not in general coincide. However, when they do,

**Definition 2.4**  *$N \leq G$  is a **normal** subgroup of  $G$  if  $gN = Ng$  for all  $g \in G$ . In this case we write  $N \trianglelefteq G$ .*

Groups where the operation is commutative are known as *abelian* groups, and clearly all subgroups are normal in this case. Normal subgroups are crucial in an important definition as follows.

**Definition 2.5** *The trivial group  $\{e\}$  and the entire group  $G$  always form normal subgroups. If these are the only normal subgroups that exist and  $G \neq \{e\}$ , then  $G$  is said to be **simple**.*

The number of left and right cosets a particular subgroup has is equal, and is also a quantity of interest.

**Definition 2.6** *The number of left and right cosets of a subgroup  $H$  in a group  $G$  is the **index** written  $[G : H]$ .*

We write  $|G|$  for the number of elements in  $G$ , known as the *order* of  $G$ . A powerful result is then,

**Theorem 2.1 (Lagrange's Theorem)** *If  $G$  is a finite group and  $H \leq G$  then  $|G| = [G : H] \cdot |H|$ .*

In particular this implies that the order of a subgroup divides the order of the group.

The complete collection of cosets of a subgroup in itself forms a new mathematical space, that of a coset space or quotient group.

**Definition 2.7** *Given  $H \leq G$  the complete collection of right cosets forms the **coset space**  $\text{cos}(G : H)$ . Given  $N \trianglelefteq G$  then the coset space denoted  $G/N$  is a group, known as a **quotient group**. The product of two cosets in a quotient group is simply the product of sets;  $(Na)(Nb) = N(aN)b = N(Na)b = N(ab)$ .*

A group element or a set of group elements may be used to generate a group.

**Definition 2.8** *The cyclic subgroup **generated** by  $x$  is  $\langle x \rangle = \{\dots x^{-1}, e, x, x^2 \dots\}$ . Given a set  $K \subset \text{Sym}(\Omega)$  then  $\langle K \rangle$  is the intersection of all the subgroups of  $\text{Sym}(\Omega)$  which contain  $K$ . It is not difficult to see that the intersection of subgroups is itself a subgroup. Equivalently  $\langle K \rangle$  is the smallest subgroup containing  $K$ .*

One of the most powerful tools in dealing with groups is the idea of mapping one group to another.

**Definition 2.9** A **homomorphism** from a group  $G$  to a group  $H$  is a mapping  $\phi : G \rightarrow H$  such that  $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$  for all  $a, b \in G$ .

Associated with homomorphisms are two important structures.

**Definition 2.10** The **kernel** of a homomorphism  $\phi : G \rightarrow H$  is the set  $\text{Ker}(\phi) = \{g \in G : \phi(g) = e\}$

**Definition 2.11** The **image** of a homomorphism  $\phi : G \rightarrow H$  is the set  $\text{Im}(\phi) = \{\phi(g) : g \in G\}$

An *isomorphism* between groups occurs if there is a bijective homomorphism between them. If there is an isomorphism between  $G$  and  $H$  we write  $G \cong H$ . An isomorphism from  $G$  to itself is an *automorphism*. The complete collection of automorphisms itself is a group, denoted  $\text{Aut}(G)$ .

### 3 Group Actions

The notion of a *group action* is very important in understanding the structure of groups.

**Definition 3.1** *Let  $G$  be a group and  $\Omega$  a set. An **action** of  $G$  on  $\Omega$  is a map  $\Omega \times G \rightarrow \Omega$ , written  $(\omega, g) \mapsto \omega^g$  satisfying;*

- *For all  $g, h \in G$  and  $\omega \in \Omega$ , we have  $(\omega^g)^h = \omega^{gh}$ .*
- *For all  $\omega \in \Omega$  we have  $\omega^e = \omega$ .*

The above defines an *right* product action. Left product actions are defined analogously from  $G \times \Omega \rightarrow \Omega$ . The main difference between left and right product actions is the order in which a product  $gh$  acts on an element of  $\Omega$ . In a left action the order is  $h$  acting first followed by  $g$ . In general only right actions will be considered, however right and left actions are essentially the same.

If a group  $G$  has an action on  $\Omega$ , then  $\Omega$  is a  $G$ -space. For permutation groups there is a very natural group action. Since a permutation of a set  $\Omega$  is simply a bijection from  $\Omega \rightarrow \Omega$ , an element  $g$  of a permutation group  $G$ , that is a subgroup of  $\text{Sym}(\Omega)$ , acts on  $\omega \in \Omega$  by  $\omega^g$  being the image of  $\omega$  under the permutation  $g$ .

As mentioned previously, all groups behave in some way like permutation groups. This is due to Cayley's theorem.

**Theorem 3.1 (Cayley's Theorem)** *Every group  $G$  is isomorphic to a permutation group of some underlying set  $\Omega$ .*

**Proof.** Let  $G$  be a group and  $\Omega = G$ . Then  $\Omega$  is a  $G$ -space with the natural action of the group product, here acting from the left. Take  $g \in G$  and define a map  $\rho_g : \Omega \rightarrow \Omega$  by  $\rho_g(\omega) = g \cdot \omega$ , for all  $\omega \in \Omega$ . Then;

$$\rho_g(\rho_{g^{-1}}(\omega)) = g \cdot (g^{-1} \cdot \omega) = (gg^{-1}) \cdot \omega = e \cdot \omega = \omega.$$

Thus the map  $\rho_g$  has a right inverse, and a similar argument shows it also has a left inverse making it a bijection and therefore a permutation. From here we construct the homomorphism  $\rho : G \rightarrow \text{Sym}(\Omega)$  defined by  $\rho(g) = \rho_g$ . To see that the map is a homomorphism we note that for all  $\omega \in \Omega$ ;

$$\rho_{gh}(\omega) = (gh) \cdot \omega = g \cdot (h \cdot \omega) = \rho_g \rho_h(\omega).$$

The kernel of this homomorphism is clearly the identity and so the homomorphism is in actual fact an isomorphism onto a subgroup of  $\text{Sym}(\Omega)$

□

The methods used in the proof above give rise to a new representation of a group.

**Definition 3.2** *The homomorphism above is called the **permutation representation** of  $G$  on  $\Omega$ . The image of the homomorphism is a permutation group denoted  $G^\Omega$ , and is known as the permutation group **induced** by  $G$  on  $\Omega$ .*

How an action moves elements of the set is important.

**Definition 3.3** *An action is **faithful** if for every non-trivial (that is, non-identity)  $g \in G$ , there exists  $\omega \in \Omega$  such that  $\omega^g \neq \omega$ .*

An important structure which comes out from group actions is the notion of an *orbit*.

**Definition 3.4** *The **orbit** of a given element  $\omega$  of a  $G$ -space  $\Omega$  is the set;*

$$\text{Orb}_G(\omega) = \omega^G = \{\omega^g : g \in G\}.$$

This structure opens up some interesting questions which go deeper into the nature of groups. How large is an orbit? How many orbits are there?

What does it mean if the orbit is all of  $\Omega$ ? The orbit of an element  $\omega$  is the set of points it can be moved to by the group action, but what about those elements of the group which do not move  $\omega$ ?

Two elements  $\alpha, \beta \in \Omega$  are in the same orbit if there exists  $g \in G$  such that  $\alpha^g = \beta$ . This induces an equivalence relation on the  $G$ -space  $\Omega$ , write  $\alpha \sim \beta$  if  $\alpha$  and  $\beta$  are in the same orbit. To check this is an equivalence relation, we check;

- Reflexivity; clearly  $\alpha \sim \alpha$  since  $\alpha^e = \alpha$ .
- Symmetry; let  $\alpha \sim \beta$  then  $\alpha^g = \beta$  for some  $g \in G$ . Then  $\beta^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^{g \cdot g^{-1}} = \alpha^e = \alpha$  implies  $\beta \sim \alpha$ .
- Transitivity; let  $\alpha \sim \beta$  and  $\beta \sim \delta$ , then  $\alpha^{g_1} = \beta$  and  $\beta^{g_2} = \delta$ , which implies  $\alpha^{g_1 \cdot g_2} = (\alpha^{g_1})^{g_2} = \delta$  which implies that  $\alpha \sim \delta$ .

Therefore the orbits of the  $G$ -space  $\Omega$  *partition*  $\Omega$ . That is either two orbits are equal or have an empty intersection, and  $\Omega$  can be expressed as the complete union of its orbits. What if there is only one orbit, comprising the entire group?

**Definition 3.5** A  $G$ -space  $\Omega$  is said to be **transitive** if  $\alpha^G = \Omega$  for any  $\alpha$ . That is, all the elements of  $\Omega$  lie in one orbit. This is equivalent to saying that a group is transitive if and only if for any distinct  $\alpha, \beta \in \Omega$  there exists  $g \in G$  such that  $\alpha^g = \beta$ .

If  $\Delta \subset \Omega$  is a union of orbits there is a natural action of  $G$  on  $\Delta$ , and so we can consider  $\Delta$  to be a  $G$ -space in its own right, in particular if  $\Delta$  is comprised of only one orbit then it is a transitive  $G$ -space. Then  $G$  induces a permutation group on  $\Delta$  by restricting the action to  $\Delta$ . This is called a transitive constituent of  $G$  and is denoted  $G^\Delta$ .

To complement the concept of an orbit is another structure known as a *stabiliser*.

**Definition 3.6** Given  $\alpha \in \Omega$  the **stabiliser** of  $\alpha$  in  $G$  is the set;

$$G_\alpha = \text{Stab}_G(\alpha) = \{g \in G : \alpha^g = \alpha\}.$$

This idea of a stabiliser will be useful in showing that transitive  $G$ -spaces look precisely like coset spaces. To do this we require a map between  $G$ -spaces much like we had group mappings, homomorphisms and isomorphisms.

**Definition 3.7** *A map  $\Phi : \Omega \rightarrow \Omega'$  between two  $G$ -spaces is a **G-morphism** if for every  $\omega \in \Omega$  and  $g \in G$ ,*

$$\Phi(\omega^g) = \Phi(\omega)^g.$$

*The  $G$ -morphism is a **G-isomorphism** if  $\Phi$  admits an inverse (which is also a  $G$ -morphism).*

Now to demonstrate that transitive  $G$ -spaces have the same appearance as coset spaces.

**Theorem 3.2** *Let  $\Omega$  be a transitive  $G$ -Space. Then  $\Omega$  is  $G$ -isomorphic to the  $G$ -space formed by the action of  $G$  on the coset space  $\text{cos}(G : G_\alpha)$  by right multiplication, for any  $\alpha \in \Omega$ .*

**Proof.** Define a map  $\Phi : \Omega \mapsto \text{cos}(G : G_\alpha)$  by  $\Phi(\omega) = G_\alpha g$  where  $g \in G$  is such that  $\alpha^g = \omega$ . Since  $\Omega$  is transitive  $g$  is guaranteed to exist. Now  $\Phi$  needs to be well defined, meaning that  $g$  is merely a representative of the coset and the choice of representative does not matter. Let  $h \in G$  be such that  $\alpha^h = \omega$ , and therefore  $\alpha^g = \alpha^h$ . Then  $G_\alpha g = G_\alpha h$  since;

$$\alpha^g = \alpha^h \quad \Leftrightarrow \quad \alpha^{gh^{-1}} = \alpha \quad \Leftrightarrow \quad gh^{-1} \in G_\alpha \quad \Leftrightarrow \quad G_\alpha g = G_\alpha h.$$

This also means that  $\Phi$  is injective. It is also surjective since every coset in the coset space is mapped to since  $\Omega$  is transitive. Hence  $\Phi$  is a bijection.

To demonstrate that  $\Phi$  is a  $G$ -morphism we must show that for any  $\omega \in \Omega$  and  $g \in G$  we have  $\Phi(\omega^g) = \Phi(\omega)^g$ . Find  $h \in G : \alpha^h = \omega$  then;

$$\Phi(\omega^g) = \Phi(\alpha^{hg}) = G_\alpha hg = \Phi(\omega)^g.$$

□

The group  $G$  is said to act *regularly* on a set  $\Omega$  if it is transitive and the stabiliser of every point in  $\Omega$  is the identity. If  $G$  acts regularly, then the action of  $G$  on  $\Omega$  is isomorphic to its action on itself (the action on itself being right multiplication) by the above theorem. In this case  $G$  also acts faithfully.

We may make a natural extension of transitivity by the following definition.

**Definition 3.8** *Let  $k \in \mathbb{N}$ . Then a  $G$ -space  $\Omega$  is  **$k$ -transitive** if for any two tuples of  $k$  distinct points  $(\alpha_1, \dots, \alpha_k)$  and  $(\beta_1, \dots, \beta_k)$  there exists  $g \in G$  such that  $\alpha_i^g = \beta_i$  for  $i \in \{1, 2, \dots, k\}$ .*

A weakening of the concept of transitivity leads to homogeneity.

**Definition 3.9** *A  $G$ -space  $\Omega$  is  **$k$ -homogenous** if for all  $\Gamma, \Delta \subseteq \Omega$  where  $|\Gamma| = |\Delta| = k$  there exists  $g \in G$  such that  $\Gamma^g = \Delta$ .*

The difference between transitivity and homogeneity is that transitivity imposes an order on the elements, homogeneity does not. Clearly a  $k$ -transitive group is necessarily  $k$ -homogenous, but the converse is not always true [3, Theorem 9.4B].

## 4 Primitivity

A group action on a set can be broken down into transitive actions. These actions themselves can be broken down into a product of transitive actions, and we may continue further until arriving at actions which cannot be further broken down. These are primitive actions.

**Definition 4.1** Let  $\Omega$  be a  $G$ -space and  $\sim$  an equivalence relation on  $\Omega$ . If  $\alpha \sim \beta \Leftrightarrow \alpha^g = \beta^g$  for all  $\alpha, \beta \in \Omega$  and for all  $g \in G$  then  $\sim$  is a **G-congruence** on  $\Omega$ . We also say that  $\sim$  is **G-invariant**. The equivalence classes of  $\sim$  are called simply the classes of the  $G$ -congruence  $\sim$ .

A *non-trivial G-congruence* is one where there is a class with more than one element, and if there is more than one class the congruence is said to be *proper*. This leads to an important theorem;

**Theorem 4.1** Let  $\Omega$  be a transitive  $G$ -space and let  $N \trianglelefteq G$ . Then the orbits of  $N$  are the classes of a  $G$ -congruence  $\sim$  on  $\Omega$ .

**Proof.** Define  $\alpha \sim \beta$  if and only if there exists  $x \in N : \alpha^x = \beta$ . Then  $\sim$  is an equivalence relation, the classes being orbits of  $N$ . Given  $\alpha \sim \beta$ , let  $x \in N$  be such that  $\alpha^x = \beta$ . If  $\sim$  is a  $G$ -congruence, we want to show that  $\alpha^g \sim \beta^g$  for  $g \in G$ .

We have  $\alpha^{xg} = \beta^g$ . Since  $N$  is normal there exists  $x' \in N : xg = gx'$ . Then  $\beta^g = \alpha^{xg} = \alpha^{gx'}$  implies that  $\alpha^g \sim \beta^g$ .

Conversely if  $\alpha^g \sim \beta^g$  then  $\alpha^{gx} = \beta^g$  for some  $x \in N$ ; so  $\alpha^{g^xg^{-1}} = \beta$  implies that  $\alpha \sim \beta$  since  $gxg^{-1} \in N$ .  $\square$

If  $\rho$  is a  $G$ -congruence and  $\alpha, \beta \in \Omega$  belong to the same  $\rho$ -class then  $\alpha$  and  $\beta$  are said to be  $\rho$ -equivalent, written  $\alpha \equiv_\rho \beta$ . Another notation to describe the  $\rho$ -class containing  $\alpha \in \Omega$  is  $\rho(\alpha) = \{\omega \in \Omega : \omega \equiv_\rho \alpha\}$ . If a  $G$ -space  $\Omega$  is transitive then all classes will be of equal size. Specifically if  $\Omega$  is transitive and finite, the size of any class is a divisor of  $|\Omega|$  since the classes partition  $\Omega$ .

We may now get a better handle on the meaning of primitivity.

**Definition 4.2** Let  $\Omega$  be a transitive  $G$ -space. Then  $\Omega$  is said to be a **primitive**  $G$ -space if there are no non-trivial (having at least one class with more than one element), proper (having more than one class)  $G$ -congruences. Thus any congruence on a primitive  $G$ -space is either trivial or has only a single class encompassing all of  $\Omega$ .

There are a number of different ways to think of primitivity, however, and the above is perhaps not the easiest one. A later theorem will provide equivalent definitions of primitivity.

The primitivity of a group is related to the transitivity of its normal subgroups, as the following theorem shows.

**Theorem 4.2** Let  $G$  be a group acting faithfully and primitively on a set  $\Omega$ . If  $N \trianglelefteq G$  and  $N \neq \{e\}$  then  $N$  is transitive.

**Proof.** The orbits of  $N$  define a  $G$ -congruence on  $\Omega$ . Since  $G$  is primitive the congruence must be either trivial or universal. It cannot be trivial, since then  $\alpha^N = \text{Orb}_N(\alpha) = \{\alpha\}$  for all  $\alpha \in \Omega$  which contradicts the action being faithful, and so we must have the universal congruence where  $\alpha^N = \text{Orb}_N(\alpha) = \Omega$  for any  $\alpha \in \Omega$  which means  $N$  is transitive on  $\Omega$ .  $\square$

At this point we introduce a useful new structure.

**Definition 4.3** The set  $\Delta \subseteq \Omega$  is a **block** if for all  $g \in G$  either  $\Delta \cap \Delta^g = \emptyset$  or  $\Delta = \Delta^g$ . A block is non-trivial if  $|\Delta| > 1$  and proper if  $\Delta \neq \Omega$ .

The subset  $\Delta \subseteq \Omega$  is said to *separate points* if for every pair of distinct  $\alpha, \beta \in \Omega$  there exists  $g \in G$  such that precisely one of  $\alpha$  or  $\beta$  is contained in  $\Delta^g$ . Clearly singleton sets (those sets which contain precisely one element) will always separate points.

Many of the above ideas are connected in the following useful theorem.

**Theorem 4.3** For a transitive  $G$ -space  $\Omega$  with  $|\Omega| > 1$  the following are equivalent statements;

1. The  $G$ -space  $\Omega$  is primitive.

2. Every non-empty proper subset of  $\Omega$  separates points.
3. The  $G$ -space  $\Omega$  has no blocks which are non-trivial and proper.
4. For all  $\alpha \in \Omega$ ,  $\text{Stab}_G(\alpha) = G_\alpha$  is a maximal subgroup of  $G$ .

**Proof.**

We prove the implications  $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$ .

$1 \Rightarrow 2$

Let  $\Delta \neq \emptyset \subset \Omega$ . For  $\alpha, \beta \in \Omega$  write  $\alpha \sim \beta$  if for all  $g \in G$ , then  $\alpha \in \Delta^g$  if and only if  $\beta \in \Delta^g$ . In fact  $\sim$  is an equivalence relation. To see this we demonstrate that  $\sim$  satisfies the following properties;

- Reflexivity; obviously  $\alpha \sim \alpha$ .
- Symmetry; if  $\alpha \sim \beta$ , then  $\alpha, \beta \in \Delta^g$  for all  $g \in G$ , hence  $\beta \sim \alpha$ .
- Transitivity; if  $\alpha \sim \beta$  and  $\beta \sim \delta$  then  $\alpha, \beta, \delta \in \Delta^g$  for all  $g \in G$  and so therefore  $\alpha \sim \delta$ .

Now we want to show that  $\sim$  is a  $G$ -congruence. Let  $\alpha \sim \beta$  and  $g \in G$ , and we would like to show that  $\alpha^g \sim \beta^g$ . Suppose  $\alpha^g \in \Delta^h$  for some  $h \in G$ . Then  $\alpha \in \Delta^{hg^{-1}}$ . Now  $\alpha \sim \beta \Rightarrow \beta \in \Delta^{hg^{-1}}$  and therefore  $\beta^g \in \Delta^h$  meaning that  $\sim$  is a  $G$ -congruence.

Here  $\Omega$  is primitive, so  $\sim$  is either trivial (all classes having one element) or universal in which case  $\Delta = \Omega$  which contradicts the assumption that  $\Delta$  is properly contained in  $\Omega$ . Therefore  $\sim$  is a trivial congruence, and  $\Delta$  separates points.

$2 \Rightarrow 3$

Let  $\Delta$  be a non-trivial block and  $\alpha \neq \beta \in \Delta$ . If  $\alpha \in \Delta^g$  then clearly  $\Delta \cap \Delta^g \neq \emptyset$  which implies  $\Delta = \Delta^g$  since  $\Delta$  is a block. Meaning that whenever  $\alpha \in \Delta^g$  we also must have  $\beta \in \Delta^g$ , that is  $\Delta$  *does not* separate points. By (2), however, all non-empty proper subsets of  $\Omega$  separate points so we deduce that the block  $\Delta = \Omega$  and  $\Omega$  has no non-trivial proper blocks.

3  $\Rightarrow$  4

Suppose  $G_\alpha \leq H \leq G$  and let  $\Delta = \alpha^H$ . Now  $\Delta$  is in actual fact a block, suppose  $\beta \in \Delta \cap \Delta^g$  for some  $g \in G$ . Then  $\beta \in \alpha^H$  and  $\beta \in \alpha^{H^g}$  which implies there exists  $h, h' \in H$  such that  $\beta = \alpha^h = \alpha^{h'g}$ . But then  $\alpha = \alpha^{h'gh^{-1}}$  implies  $h'gh^{-1} \in G_\alpha \leq H$  which implies  $g \in H$  therefore  $\Delta^g = \Delta$  which is sufficient to show that  $\Delta$  is a block. By (3) this means that either  $\Delta = \{\alpha\}$  or  $\Delta = \Omega$ . In the former  $H$  stabilises  $\alpha$  and so  $G_\alpha = H$ . In the second case  $\alpha^H = \Omega$  making  $H$  transitive on  $\Omega$ . Then in this case given  $\beta \in \Omega$  let  $h_\beta \in H$  be such that  $\alpha^{h_\beta} = \beta$ . Since  $H$  is transitive, such a  $h_\beta$  is guaranteed to exist. Then;

$$G = \bigcup_{\beta \in \Omega} G_\alpha h_\beta \leq H$$

Therefore  $H = G$ , and so  $G_\alpha$  is a maximal subgroup as no proper subgroup contains it but is not equal to it.

4  $\Rightarrow$  1

Given a  $G$ -congruence  $\sim$  we wish to show that it is either trivial or universal. Let  $\Delta$  be the  $\sim$ -class containing  $\alpha$  and let  $H$  be the *setwise stabiliser* of  $\Delta$  in  $G$ ;

$$H = G_{\{\Delta\}} = \{g \in G : \Delta^g = \Delta\}.$$

Given  $g \in G_\alpha$  and  $\delta \in \Delta$  then  $\delta \sim \alpha$  which implies  $\alpha = \alpha^g \sim \delta^g$  which means  $G_\alpha \leq H$ . By 4.  $G_\alpha$  is maximal and so either  $H = G_\alpha$  in which case  $\Delta = \{\alpha\}$  and the congruence is trivial, or  $H = G$  and then  $\Delta = \Omega$  and the congruence is universal.  $\square$

As with transitivity, there is an extension of primitivity;

**Definition 4.4** Let  $k \in \mathbb{N}$ . A group  $G$  acting on  $\Omega$  is **k-primitive** if it is  $k$ -transitive and for all distinct  $\alpha_1, \dots, \alpha_{k-1} \in \Omega$  the pointwise stabilisers  $G_{\alpha_1, \dots, \alpha_{k-1}}$  are primitive on  $\Omega \setminus \{\alpha_1, \dots, \alpha_{k-1}\}$

We state, without proof, a theorem connecting the extensions of primitivity and transitivity [2, Lemma 4.10];

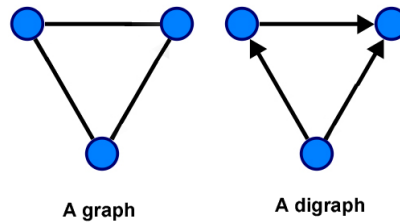
**Theorem 4.4** A  $k$ -transitive group is at least  $(k-1)$ -primitive.

## 5 Graphs

A short section on graphs mainly concerned with laying down some core definitions.

**Definition 5.1** A **graph**  $\Gamma(V, E)$  consists of a set  $V$  of **vertices** and a set of **edges**  $E$ . In a graph the edge set consists of unordered pairs of vertices. However a **digraph** has as an edge set pairs of ordered vertices, in this case the edges are referred to as **arcs** and an arc goes from one vertex in  $V$  to another.

A simple diagram is however more illuminating than a difficult definition.



**Definition 5.2** A **path** in a graph  $\Gamma$  from  $\alpha$  to  $\beta$  is a sequence of vertices;

$$\alpha = \alpha_0, \alpha_1, \dots, \alpha_n = \beta$$

Such that  $\{\alpha_i, \alpha_{i+1}\} \in E$ . If  $\Gamma$  is a digraph then a **dipath** is a similar sequence of vertices with the caveat that  $(\alpha_i, \alpha_{i+1})$  is an arc in  $E$ .

**Definition 5.3** The **length** of a path is the number of edges it contains. The **distance** between  $\alpha$  and  $\beta$  is the length of the shortest path between them.

**Definition 5.4** A graph (or digraph) is said to be **connected** if for any distinct  $\alpha, \beta \in V$  there is a path (or dipath) between  $\alpha$  and  $\beta$ . A digraph is **strongly connected** if there exists a path from  $\alpha$  to  $\beta$  as well as from  $\beta$  to  $\alpha$ .

**Definition 5.5** *The diameter of a graph is the length of the greatest distance between any two vertices.*

A finite graph having finite diameter is equivalent to the graph being connected. If the diameter of a graph is 1, then the graph is complete, that is every vertex is adjacent to every other vertex.

## 6 Suborbits, orbitals and orbital graphs

Let us quickly introduce two new definitions, that of a suborbit and that of an orbital. If  $\Omega$  is a transitive  $G$ -space, then;

**Definition 6.1** *Let  $\alpha \in \Omega$ . The stabiliser of  $\alpha$ ,  $G_\alpha$  also acts on  $\Omega$ . The orbits of  $G_\alpha$  are called the **suborbits** of  $G$ .*

**Definition 6.2** *The group  $G$  also acts on  $\Omega \times \Omega$  by the action  $(\omega_1, \omega_2)^g = (\omega_1^g, \omega_2^g)$ . The orbits of  $G$  on  $\Omega^2$  are the **orbitals** of  $G$ .*

Since  $G$  is transitive on  $\Omega$ , the subset  $\Delta_0 = \{(\omega, \omega) : \omega \in \Omega\}$  is always an orbital and is called the *diagonal orbital* of  $G$ . The set  $\{\alpha\}$  is always a  $G_\alpha$ -orbit and is known as the *trivial suborbit* of  $G$ .

Orbitals and suborbits are connected in the following theorem;

**Theorem 6.1** *Let  $\Omega$  be a transitive  $G$ -space and let  $\alpha \in \Omega$ . There is a natural bijection between the orbits of  $G_\alpha$  on  $\Omega$  and the  $G$ -orbits on  $\Omega^2$ . The trivial suborbital corresponds to the diagonal orbital.*

**Proof.** Given  $\Delta \in \Omega^2$  we define  $\Delta(\alpha) \subseteq \Omega$  by;

$$\Delta(\alpha) = \{\beta \in \Omega : (\alpha, \beta) \in \Delta\}$$

Then let  $\Delta$  be an orbital. Now  $\Delta(\alpha) \neq \emptyset$  since  $G$  is transitive. Let  $\beta_1, \beta_2 \in \Delta(\alpha)$ . Then there exists  $g \in G$  such that  $(\alpha, \beta_1)^g = (\alpha, \beta_2)$  since  $\Delta$  is an orbital. However  $g$  fixes  $\alpha$  therefore  $g \in G_\alpha$  and  $\beta_1^g = \beta_2$ . Therefore  $\Delta(\alpha)$  is equal to an orbit of  $G_\alpha$  on  $\Omega$ . The assignment  $\Delta \mapsto \Delta(\alpha)$  is a bijection between the orbitals and  $G_\alpha$ -orbits.

□

From orbitals we may construct orbital graphs and orbital digraphs;

**Definition 6.3** *Let  $G$  be a group acting on a set  $\Omega$  and let  $\Delta$  be an orbital of  $G$ . The **orbital digraph** of  $G$  with respect to  $\Delta$  is the digraph having  $\Omega$  as a vertex set and  $\Delta$  as its edge set. The **orbital graph** is simply the same graph but without the direction imposed upon the arcs.*

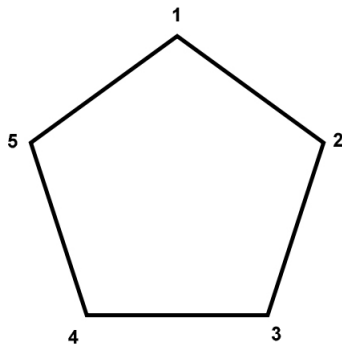
As a simple concrete example consider the cyclic group of five elements  $C_5 = \{1, 2, 3, 4, 5\}$  acting on itself by translation. If we take  $\Delta = (1, 2)$  then we see that;

$$(1, 2)^1 = (1^1, 2^1) = (1, 2)$$

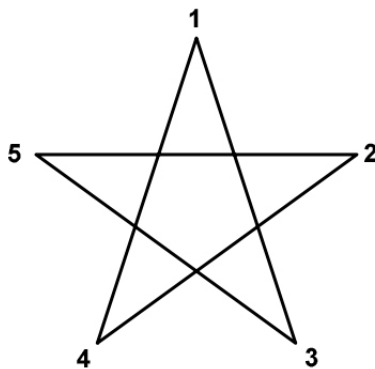
$$(1, 2)^2 = (2, 3)$$

...

So the final orbital graph looks like this;



Now if we take a different orbital we shall generate another graph. This time we take  $\Delta = (1, 3)$  we produce a pentagram as the orbital graph;



Notice that in both cases the graph is connected and the diameter of the graph is 2. Moreover, the two graphs are isomorphic.

Two vertices being connected induces an equivalence relation, write  $\alpha \sim \beta$  if  $(\alpha, \beta)$  is a directed edge. Not only that, but if  $\Gamma$  is the orbital graph of a  $G$ -orbital  $\Delta$ , then  $\sim$  is a  $G$ -congruence. Suppose  $\alpha \sim \beta$ , that is,

$$\alpha = \alpha_0, \alpha_1, \dots, \alpha_n = \beta$$

is a path in  $\Gamma$ . Then given  $g \in G$  the following is also a path.

$$\alpha^g = \alpha_0^g, \alpha_1^g, \dots, \alpha_n^g = \beta^g$$

From  $\alpha^g$  to  $\beta^g$ , since  $(\alpha_i, \alpha_{i+1}) \in \Delta$  which implies  $(\alpha_i^g, \alpha_{i+1}^g) = (\alpha_i, \alpha_{i+1})^g \in \Delta^g = \Delta$ , meaning that  $\sim$  is also a  $G$ -congruence. The classes of which are called the *strong components* of  $\Gamma$ .

A graph is said to be *connected* if there is a path connecting any two distinct vertices. A theorem from Higman [2, Theorem 5.7] relates the primitivity of a transitive  $G$ -space and the connectedness of its orbital graphs.

**Theorem 6.2** *Let  $\Omega$  be a transitive  $G$ -space. Then  $\Omega$  is primitive if and only if for every orbital  $\Delta$  except the diagonal orbital, the orbital graph of  $\Delta$  is connected.*

**Proof.**

First assume primitivity. The relation  $\sim$  described above is a  $G$ -congruence, so must be either trivial or universal. Since  $\Delta$  is not equal to the diagonal orbital  $\Delta_0 = \{(\omega, \omega) : \omega \in \Omega\}$ , then  $\Delta = (\alpha, \beta)^G$  where  $\alpha \neq \beta$ . Since  $\alpha \neq \beta$  the relation is not trivial, therefore it must be universal which implies any two vertices are joined by a path, and hence the graph is connected.

Conversely assume that every non-trivial orbital graph is connected, and let  $\Gamma \in \Omega$  be a non-trivial block with  $\alpha, \beta \in \Gamma$  such that  $\alpha \neq \beta$ . The orbital graph of the orbital  $(\alpha, \beta)^G$  is connected. If  $\Gamma \neq \Omega$  then there exists  $g \in G$  such that precisely one of  $\alpha^g$  or  $\beta^g \in \Gamma$ . This corresponds to the fact that if  $\Gamma \neq \Omega$  there must be an edge in the graph with one vertex in  $\Gamma$  and the other outside. But this contradicts  $\Gamma$  being a block. Therefore  $\Gamma = \Omega$  and so  $\Omega$  is primitive (from Theorem 4.3).  $\square$

For finite graphs finite diameter is equivalent to connectedness. For an infinite family of finite graphs, their having a uniformly bounded diameter is a strong form of connectedness. Some families of finite primitive permutation groups which have orbital graphs with a uniform finite upper bound have been described [1]. However explicit bounds for more select families of groups have not yet been developed.

## 7 The O’Nan-Scott Theorem

An exceptionally powerful theorem, described in [4], classifies finite primitive permutation groups into five classes. The proof is beyond our scope and the language used to describe the classes somewhat technical and will need some discussion. Firstly the socle of a group must be defined. The definitions of a normal subgroup and minimal subgroup have been given in Section 2, one defines a minimal *normal* subgroup similarly, but also required are,

**Definition 7.1** *The socle of a group  $G$  is the group generated by the set of all minimal normal subgroups of  $G$  and is denoted  $\text{soc}(G)$*

Although in the definition the socle is a group generated by minimal normal subgroups, in fact it can be viewed as a direct product of some or all of these subgroups.

**Theorem 7.1** *Let  $G$  be a finite group. Then the following hold.*

1. *If  $K$  is a minimal normal subgroup of  $G$ , and  $L$  is any normal subgroup of  $G$ , then either  $K \leq L$  or  $\langle K, L \rangle = K \times L$ .*
2. *There exist minimal normal subgroups  $K_1, \dots, K_m$  of  $G$  such that  $\text{soc}(G) = K_1 \times \dots \times K_m$*
3. *Every minimal normal subgroup  $K$  of  $G$  is a direct product  $K = T_1 \times \dots \times T_k$  where the  $T_i$  are simple normal subgroups of  $K$  which are conjugate under  $G$ .*

**Proof.**

1. The group  $K \cap L$  is normal in  $G$ , and since  $K$  is minimal either  $K \cap L = K \leq L$  or  $K \cap L = 1$ . In the latter case  $\langle K, L \rangle = KL = \{kl : k \in K, l \in L\} = K \times L$ . This is true because elements from  $K$  and  $L$  commute, and so any string  $k_1 l_1 k_2 l_2 \dots k_n l_n$  can be written as  $k'l'$ .

2. Because  $G$  is finite we may find a set  $S = \{K_1, \dots, K_m\}$  of minimal normal subgroups of  $G$  which is maximal with respect to  $H = \langle S \rangle$ , being a direct product of the  $K_i$ . We require to show that  $H$  is the socle, which follows if  $H$  contains all minimal normal subgroups of  $G$ . Let  $K$  be a minimal normal subgroup of  $G$ , then by (1) either  $K \leq H$  or  $\langle K, H \rangle = K \times H$ . The latter option is impossible due to the choice of  $S$ , therefore  $H$  contains all the minimal normal subgroups and is necessarily the socle of  $G$ .
3. Let  $T$  be a minimal normal subgroup of  $K$ . The conjugates  $g^{-1}Tg$  of  $T$  where  $g \in G$  are also minimal normal subgroups of  $K$ . Pick a set  $\{T_1, \dots, T_k\}$  of these conjugates which is maximal with respect to  $L = \langle T_1, \dots, T_k \rangle$  is a direct product of the  $T_i$ . By an analogous argument in (2),  $L$  contains all the conjugates of  $T$  under  $G$ . This implies  $L \trianglelefteq G$ . Now  $K$  is a minimal normal subgroup and  $1 \neq L \leq K$  and so therefore  $K = L = T_1 \times \dots \times T_k$ . For each  $T_i$  their normal subgroups are clearly normal in  $K$ , and then the minimality of  $T_i$  shows that it is a simple group.

□

Assertions (2) and (3) of the previous theorem together with the fact that conjugate subgroups are isomorphic means that the socle of a primitive permutation group is isomorphic to  $T^k$  where  $T$  is a simple group.

One of the classes that the O’Nan-Scott divides finite primitive permutation groups into are *affine* groups. Here  $\text{soc}(G) \cong T^k$  where  $T = C_p$  the cyclic group of  $p$  elements where  $p$  is a prime. The socle is the unique minimal normal subgroup of  $G$  and is regular on  $\Omega$  where  $|\Omega| = n = p^k$ . Here  $G$  is a subgroup of the affine group  $\text{AGL}(k, p)$  with the socle being the translation group.

This is best understood in terms of geometry. The affine group  $\text{AGL}(k, p)$  can be understood in terms of the  $k$ -dimensional vector space over the finite field of  $p$  elements;  $\mathbb{F}_p$ . Here  $\Omega = \mathbb{F}_p^k$  and the group operations are affine transformations. These are best understood in terms of block matrices. These are matrices of the following form;

$$\left( \begin{array}{c|c} M & v \\ \hline 0 & 1 \end{array} \right)$$

Where  $M \in \text{GL}(k, p)$  and  $v \in \mathbb{F}_p^k$ . In terms of  $\text{AGL}(k, p)$ , the matrix is a square matrix of degree  $k + 1$ . Here  $M$  is a matrix contained in  $\text{GL}(k, p)$  which are those invertible  $k$ -degree square matrices over  $\mathbb{F}_p$ . A matrix being invertible is equivalent to it having a non-zero determinant, which is equivalent to the column vectors being linearly independent; that is no particular column vector can be written as a linear combination of the others. Here  $v$  is a  $k$ -dimensional column vector.

The elements of the group  $\text{AGL}(k, p)$  have a natural action on the  $k$ -dimensional column vectors over  $\mathbb{F}_p$  by left multiplication. However the elements of  $\text{AGL}(k, p)$  are represented as  $k + 1$ -dimensional square matrices, to counter this discrepancy in dimension we write the column vectors the group is acting on as  $k + 1$ -dimensional vectors with the last superfluous element being always 1. The group operation is matrix multiplication, which for  $k \geq 1$  is non-commutative making this group nonabelian.

For a concrete example let us look at  $\text{AGL}(2, 3)$ . The size of the group is  $|\text{AGL}(2, 3)| = |\text{GL}(2, 3)| |\mathbb{F}_3^2| = (3^2 - 1)(3^2 - 3)(3^2) = 432$ . The group acts on the following set.

$$\mathbb{F}_3^2 \cong \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} \right\}.$$

Having nine elements in total.

To construct the orbital graph, we first choose as a starting edge,

$$\Delta = \left( \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right).$$

To see how the elements of  $\text{AGL}(2, 3)$  act on these two vectors we perform the action explicitly.

$$\begin{pmatrix} a & b & x \\ c & d & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b & x \\ c & d & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a+x \\ c+y \\ 1 \end{pmatrix}$$

The only restriction here is that  $ad - bc \neq 0$ . Where can this pair be mapped to using the action of a group element? Suppose we want to find a group element that moves the pair to the new distinct pair (and it must be a distinct pair, no group element can map two distinct points to the same single point),

$$\left( \begin{pmatrix} \alpha \\ \beta \\ 1 \end{pmatrix}, \begin{pmatrix} \gamma \\ \delta \\ 1 \end{pmatrix} \right).$$

Then we can simply let  $x = \alpha$  and  $y = \beta$  and then  $a = \gamma - \alpha$  and  $c = \delta - \beta$ .

$$\begin{pmatrix} \gamma - \alpha & b & \alpha \\ \delta - \beta & d & \beta \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \gamma - \alpha & b & \alpha \\ \delta - \beta & d & \beta \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \\ 1 \end{pmatrix}.$$

Since the new pair are distinct  $a = \gamma - \alpha$  and  $c = \delta - \beta$  cannot both be zero, and here  $b$  and  $d$  are free choices that do not affect how the matrix moves the vectors, and so can be chosen to ensure that  $ad - bc \neq 0$ . Thus our original pair can be mapped to any other pair of distinct elements, meaning the orbital graph is *complete* and the diameter is 1.

In this construction we have used the fact that if a pair of elements can be mapped to any other pair, then the orbital graph is complete. This is equivalent to the group being 2-transitive if the pairs are ordered, or 2-homogenous if not. In this case the argument we used shows that  $\text{AGL}(2, 3)$  is 2-transitive. The argument is largely independent of dimension, so it is reasonable to ask whether all the complete affine groups are 2-transitive. This is indeed true [3, p.244], and so this is rather a dead

end since all the orbital graphs will have a diameter of one. Instead we look towards the projective special linear group to make progress.

This was an investigation into one branch of the classes that the O’Nan-Scott theorem divides primitive permutation groups into. The theorem however formulates further classes described as follows. The language required to fully describe these classes is technical however, and is not particularly relevant so only the briefest of descriptions is provided. For full details refer to [4].

- *Almost simple groups.* Here  $\text{soc}(G) \cong T$  where  $T$  is a nonabelian simple group.
- Here  $\text{soc}(G) \cong T^k$  where  $k \geq 2$  and  $T$  is a nonabelian simple group. We branch into three subclasses,
  - *Simple diagonal action*
  - *Product action*
  - *Twisted wreath action*

## 8 The Projective Special Linear Groups

The projective special linear group is most easily understood as a quotient group. The general linear group  $\text{GL}(k, p)$  is the group of  $k$ -dimensional invertible matrices over  $\mathbb{F}_p$ . The *special* linear group is a subgroup of the above formed by demanding that the determinant of the matrix be equal to one. The projective special linear group is created by forming the quotient group of  $\text{SL}(k, p)$  by its centre. For the time being we set  $k = 2$  and take  $p > 2$  a prime. Then the centre of  $\text{SL}(2, p)$  is simply,

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

This can be thought of as disregarding the difference between positive and negative and so  $\text{PSL}(2, p)$  is half the size of  $\text{SL}(2, p)$ . Now  $\text{PSL}(2, p)$  has a natural action on first order projective space  $\mathbb{P}^1(\mathbb{F}_p)$  which is best described as the following space,

$$\mathbb{P}^1(\mathbb{F}_p) = \left\{ \begin{pmatrix} x \\ 1 \end{pmatrix} : x \in \mathbb{F}_p \right\} \cup \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

by left multiplication. However this is another 2-transitive action [5], but it is not the only action that exists. Instead we look at an action formed when elements of  $\text{PSL}(2, p)$  act on the coset space formed by  $\text{PSL}(2, p)$  and one of its maximal subgroups. The maximal subgroup we are interested in is,

$$M = \left\langle \left\{ \overline{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}} : \lambda \in \mathbb{F}_p \setminus \{0\} \right\} \cup \left\{ \overline{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}} \right\} \right\rangle$$

Here  $M$  is a *dihedral* group. To summarise let  $G = \text{PSL}(2, p)$  and let  $\Omega = \text{cos}(G : M)$  then  $G$  acts on  $\Omega$ . The size of  $G$  and  $\Omega$  are of interest,

$$|G| = |\text{PSL}(2, p)| = \frac{|\text{SL}(2, p)|}{2} = \frac{1}{2} \cdot \frac{|\text{GL}(2, p)|}{p-1} = \frac{1}{2} \cdot \frac{(p^2-1)(p^2-p)}{p-1} = \frac{(p+1)p(p-1)}{2},$$

$$|M| = \frac{p-1}{2} \cdot 2 = p-1,$$

$$|\Omega| = \frac{|G|}{|M|} = \frac{(p+1)p}{2}.$$

We are now able to use the software Magma to computationally investigate this group action.

## 9 Computations using Magma

To quote the developers themselves;

*Magma is a large, well-supported software package designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics. It provides a mathematically rigorous environment for computing with algebraic, number-theoretic, combinatoric, and geometric objects.*

Magma's user interface is minimal and instructions are written in a simple command prompt window using intuitive syntax. With a large number of inbuilt functions one can write programs in Magma quickly and easily. Some of the most useful functions to us are outlined as follows.

- **PSL(k,p)**; constructs the projective special linear group with given parameters.
- **MaximalSubgroups(G)**; produces all the maximal subgroups of a group  $G$  up to conjugation.
- **Index(G, H)**; gives the index of the subgroup  $H$  in the group  $G$ .
- **CosetImage(G, H)**; constructs the image of  $G$  given by its action on the (right) coset space of  $H$  in  $G$ . The coset space is identified as  $\{1, 2, \dots\}$ .
- **Stabilizer(G, y)**; constructs the subgroup of  $G$  which stabilises the element  $y \in \Omega$ .
- **Orbits(G)**; produces all the orbits of  $G$  with its natural action on the set  $\Omega$ .
- **Degree(G)**; returns the permutation degree of  $\Omega$ .
- **OrbitalGraph(G, x, {y})**; constructs the orbital graph of the group  $G$  from  $\Delta = (x, y)$ .
- **Diameter( $\Gamma$ )**; returns the diameter of the graph  $\Gamma$ .

Magma in general uses the permutation representation when storing groups as this allows more efficient computation. However it means that it is sometimes difficult to describe groups which are more readily understood in a different manner, for example  $\text{PSL}(2, p)$  is better understood as a matrix group than a permutation group. Specifically one difficulty here is in catching the maximal subgroup  $M$  described in the previous chapter. However, since we know the index of  $M$  in  $G = \text{PSL}(2, p)$  is  $\frac{p(p+1)}{2}$  we can locate the desired subgroup by checking its index. If there is more than one subgroup of the desired index however, it will be difficult to know which corresponds to  $M$ .

The following is the entire code of a preliminary Magma program to investigate the orbital graphs associated to  $\text{PSL}(2, p)$ .

```

Primenumbers := [];
p := 3;
while p lt 50 do
  Include(~Primenumbers,p);
  p := NextPrime(p);
end while;

print "The orbital graphs associated to PSL(2,p)";
print "for the following p will be investigated:";
print Primenumbers;
print "";

for p in Primenumbers do
  print "-----";
  print "Considering p = ",p;
  G := PSL(2,p);
  max := MaximalSubgroups(G);
  Max := [];
  for X in max do
    if Index(G,X'subgroup) eq p*(p+1)/2 then
      Include(~Max,X'subgroup);
    end if;
  end for;
  print "Number of maximal subgroups of wanted index: ", #Max;
  print "";
end for;

```

```

for i in [1..#Max] do
  print "Maximal Subgroup # ",i;
  H := CosetImage(G,Max[i]);
  Diameters := {};
  for j in [2..Degree(H)] do
    OGraph := OrbitalGraph(H,1,{j});
    Include(~Diameters,Diameter(OGraph));
  end for;
  print "Diameters: ", Diameters;
  print "";
end for;
end for;

```

Of course those unfamiliar with Magma it is not necessarily completely transparent as to what this program does. Splitting into sections and describing each part will help give a better idea of what's happening.

```

Primenumbers := [];
p := 3;
while p lt 50 do
  Include(~Primenumbers,p);
  p := NextPrime(p);
end while;

```

This produces a set called Primenumbers. The 'while' loop begins at  $p = 3$  and keeps adding the next prime in sequence to the set until a prime larger than 50 is encountered and the loop terminates.

```

print "The orbital graphs associated to PSL(2,p)";
print "for the following p will be investigated:";
print Primenumbers;
print "";

```

This simply prints useful information to the screen.

```

for p in Primenumbers do
  print "-----";

```

```

print "Considering p = ",p;
G := PSL(2,p);
max := MaximalSubgroups(G);
Max := [];
for X in max do
  if Index(G,X'subgroup) eq p*(p+1)/2 then
    Include(~Max,X'subgroup);
  end if;
end for;
print "Number of maximal subgroups of wanted index: ", #Max;
print "";

```

This begins the main body of the program. A for loop is set up that runs through every element in the set 'Primenumbers'. The required  $\text{PSL}(2, p)$  is generated as are its maximal subgroups. Magma then runs through all the maximal subgroups to determine which has the desired index of  $\frac{p(p+1)}{2}$  and such subgroups are entered into a new set 'Max'. Here we print to screen the number of elements there are in Max, that is how many maximal subgroups of desired order there are, since as described above if there is more than one we cannot tell as yet which corresponds to the desired subgroup.

```

for i in [1..#Max] do
  print "Maximal Subgroup # ",i;
  H := CosetImage(G,Max[i]);
  Diameters := {};
  for j in [2..Degree(H)] do
    OGraph := OrbitalGraph(H,1,{j});
    Include(~Diameters,Diameter(OGraph));
  end for;
  print "Diameters: ", Diameters;
  print "";
end for;
end for;

```

This completes the program. Magma defines  $H$  to be the permutation group  $G$  on  $\text{cos}(G : \text{Max}[i])$  regarded as  $\Omega = \{1, 2, \dots |G : \text{Max}[i]|\}$ . The orbital graph of this action is produced for  $\Delta = (1, i)$  where  $i$  runs

through every other possible point. The diameter of each orbital graph is then calculated and entered into a new set 'Diameters' which is then printed to screen.

This program produces the following output.

```
-----  
Considering p = 3  
Number of maximal subgroups of wanted index: 0  
  
-----  
Considering p = 5  
Number of maximal subgroups of wanted index: 0  
  
-----  
Considering p = 7  
Number of maximal subgroups of wanted index: 0  
  
-----  
Considering p = 11  
Number of maximal subgroups of wanted index: 0  
  
-----  
Considering p = 13  
Number of maximal subgroups of wanted index: 2  
  
Maximal Subgroup # 1  
Diameters: { 2, 3, 4, 5 }  
  
Maximal Subgroup # 2  
Diameters: { 3, 4 }  
  
-----  
Considering p = 17  
Number of maximal subgroups of wanted index: 1  
  
Maximal Subgroup # 1  
Diameters: { 3, 4, 7 }  
  
-----  
Considering p = 19
```

Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 2, 3, 4 }

-----  
Considering p = 23  
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 2, 3, 4 }

-----  
Considering p = 29  
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 3, 4 }

-----  
Considering p = 31  
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 2, 3, 4 }

-----  
Considering p = 37  
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 3 }

-----  
Considering p = 41  
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1  
Diameters: { 3, 4 }

```

-----
Considering p = 43
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1
Diameters: { 2, 3, 4 }

```

```

-----
Considering p = 47
Number of maximal subgroups of wanted index: 1

Maximal Subgroup # 1
Diameters: { 2, 3, 4 }

```

Already things of interest appear. Notice that  $\text{PSL}(2, p)$  does not have the desired maximal subgroup at all for primes up to 11, and for  $p = 13$  has two whilst all the others produce (fortunately) just one. Also notice that all the orbital graphs for  $p = 37$  have diameter 3, whilst in all other cases there are at least two diameters for the different orbital graphs. They are however all connected (Magma returns  $-1$  for the diameter of an unconnected graph) which fits with this action being primitive.

However this is not a particularly efficient program. Every single orbital graph is generated, and most of them will be isomorphic to each other as noted in the simple example of the cyclic group given in section 6. It would be profitable, especially if we wish to investigate the orbital graphs for large primes, to streamline the program. We introduce the following code into the program.

```

Vertices := [];
S := Stabilizer(H,1);
Paths := Orbits(S);
for Path in Paths do
  if Path ne {1} then
    Include(~Vertices,SetToSequence(Path)[1]);
  end if;
end for;
print "Number of orbital graphs to check: ", #Vertices;
print "rather than ", Degree(H);
print "";

```

```

for j in Vertices do
  OGraph := OrbitalGraph(H,1,{j});
  Include(~Diameters,Diameter(OGraph));
end for;
print "Diameters: ", Diameters;
print "";
end for;
end for;

```

Since the vertex 1 is always a part of the starting edge of the orbital graph we generate, we find the stabiliser of the point 1 in the group  $H$ , those elements which do not move 1. The orbits of these elements are then found. The first element from each orbit is then added to the set 'Vertices'. When the orbital graphs are generated, the initial edge has one vertex being 1, and an element from the set 'Vertices' forms the second vertex. In this way calculating the diameters of isomorphic orbital graphs is avoided, since if  $\alpha, \beta$  were in the same orbit of a stabiliser of 1 then the graphs generated by  $\{1, \alpha\}$  and  $\{1, \beta\}$  would be isomorphic.

How much of a benefit does this provide? Magma is also able to time how long it takes to perform its calculations. The original program takes 276 seconds (4 minutes and 19 seconds) to calculate the diameters for primes up to 50. The improved program however takes only 8 seconds. The improvement is very significant!

With this program we are able to compute diameters associated to orbital graphs for  $\text{PSL}(2, p)$  for larger primes. The following table lists the results for the primes up to 200.

Prime	# of desired subgroups	# of graphs to check	rather than	Diameters
3	0	N/A	N/A	N/A
5	0	N/A	N/A	N/A
7	0	N/A	N/A	N/A
11	0	N/A	N/A	N/A
13	2	10,11	91	{2,3,4,5}{3,4}
17	1	14	153	{3,4,7}
19	1	15	190	{2,3,4}
23	1	18	276	{2,3,4}
29	1	23	435	{3,4}
31	1	24	496	{2,3,4}
37	1	29	703	{3}
41	1	32	861	{3,4}
43	1	33	946	{2,3,4}
47	1	36	1128	{2,3,4}
53	1	41	1431	{3}
59	1	45	1770	{2,3,4}
61	3	40,47,40	1891	{2,3,4,5,6}{3}{2,3,4,5,6}
67	1	51	2278	{2,3,4}
71	1	54	2556	{2,3}
73	1	56	2701	{3,4}
79	1	60	3160	{2,3}
83	1	63	3486	{2,3,4}
89	1	68	4005	{3,4}
97	1	74	4753	{3,4}
101	1	77	5151	{3}
103	1	78	5356	{2,3,4}
107	1	81	5778	{2,3}
109	1	83	5995	{3}
113	1	86	6441	{3,4}
127	1	96	8128	{2,3}
131	1	99	8648	{2,3,4}
137	1	104	9453	{3,4}
139	1	105	9730	{2,3}
149	1	113	11175	{3}
151	1	114	11476	{2,3}
157	1	119	12403	{3}
163	1	123	13366	{2,3}
167	1	126	14028	{2,3}
173	1	131	15051	{3}

Prime	# of desired subgroups	# of graphs to check	rather than	Diameters
179	1	135	16110	{2,3}
181	1	137	16471	{3}
191	1	144	18336	{2,3}
193	1	146	18721	{3,4}
197	1	149	19503	{3}
199	1	150	19900	{2,3}

With the available computing resources no further data could be gathered, calculating orbital graphs for primes larger than 199 simply takes an impractical amount of time. However already from this data we begin to notice interesting patterns which may direct our investigation. One immediate interpretation is that, excluding small primes, the following is true,

- The diameter set  $\{3\}$  occurs precisely for  $p \equiv 5 \pmod{8}$ .
- The diameter set  $\{3,4\}$  occurs precisely for  $p \equiv 1 \pmod{8}$ .
- The diameter set  $\{2,3\}$  or  $\{2,3,4\}$  occurs for  $p \equiv 3 \pmod{4}$ .
- Diameter set  $\{2,3,4\}$  is rare.

The diameter set  $\{2,3,4\}$  is particularly notable because whilst it appears frequently for small primes, occurrences rapidly taper off for large primes. Perhaps there are only finitely many cases?

From this point there are two main possibilities for progress. One option is to obtain more data, particularly regarding primes congruent to 3 modulo 4, which would guide our mathematical approach. This would require considerable streamlining of the current program and most likely a more indirect approach than the current method. Alternatively one could aim to proceed without use of computational techniques but begin to try and prove things in order to get a better handle on the mathematical reasons for the observed data.

## 10 Conclusion

Due to time constraints no further investigation is possible. This is slightly frustrating as the computations revealed potentially fruitful avenues of research. However in the short time available good progress was made into this particular mathematical problem, and provides a good introduction as to the directions where this kind of mathematics can be taken. In particular this report is easily accessible to all with only the slightest mathematical background and I feel this property is of some merit, particularly to those unfamiliar but interested in the field of group theory. In all this project achieved most of what it set out to do.

## References

- [1] M.W. Liebeck, D. Macpherson and K. Tent, *Primitive permutation groups of bounded orbital diameter*, to appear in Proc. London Math. Soc., advanced online access, 2009.
- [2] M. Bhattacharjee, D. Macpherson, R.G. Möller and P.M. Neumann, Notes on infinite permutation groups, Hindustan Book Agency, New Delhi, 1997.
- [3] J.D. Dixon and B. Mortimer, Permutation Groups, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.
- [4] M.W. Liebeck, C.E. Praeger and J. Saxl, *On the ONan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. (Series A) **44** (1986), p. 389–396
- [5] T. Rowland and E.W. Weisstein, Transitive group, from MathWorld, a Wolfram Web Resource, <http://mathworld.wolfram.com/TransitiveGroup.html>