

Orbital Diameters of Primitive Permutation Groups

A thesis submitted for the degree of
Doctor of Philosophy in Mathematics by

Atiqa Sheikh

a.sheikh13@imperial.ac.uk

Supervisor: Professor Martin W. Liebeck

Department of Mathematics
Imperial College London

February 2018

Declaration of Originality

I hereby declare that the thesis and the work done within it is entirely my own. Where the work of others has been used, this has been appropriately referenced.

Copyright Declaration

The copyright of the thesis rests with the author and is made available under a Creative Commons Attribution Non-Commercial No Derivatives licence. Researchers are free to copy, distribute or transmit the thesis on the condition that they attribute it, that they do not use it for commercial purposes and that they do not alter, transform or build upon it. For any reuse or redistribution, researchers must make clear to others the licence terms of this work.

Acknowledgements

First and foremost, I would like to express my sincerest gratitude to Professor Martin W. Liebeck for supervising the doctoral studies which have led to the production of the thesis. In particular, I would like to thank Martin for introducing me to the topic of the thesis which I have found immensely interesting to study over the duration of the course, for sharing his expert knowledge of the subject with me, and for skilfully answering the countless mathematical questions that I have asked him. I also appreciate Martin's comments and feedback on my written work and mathematical ideas.

I would like to thank the Mathematics Department at Imperial College London for having awarded me with a PhD studentship to pursue my research, and the support staff in the Mathematics Department for always being so helpful and friendly. I would also like to thank the libraries at Imperial, UCL, Birkbeck, City, and Senate House for providing study spaces where I have spent most of the 4 years of the PhD.

I thank my mother Kishwar and my sister Aleen for supporting me throughout the studies. In particular, I thank my mother for all the love and for preparing packed lunches for me on numerous occasions. I thank my sister for discussing and helping me solve several mathematical problems that I have struggled with, and for encouraging me to keep up with our dance and vocal practises amongst the busy schedule. Lastly, a very special thanks to my late father, Fayyaz.

Abstract

Let G be a transitive permutation group acting on a finite set X . Recall that G is primitive if there are no non-trivial equivalence relations on X which are preserved by G . An *orbital graph* of G is a graph with vertex set X and edges $\{x, y\}$, where (x, y) belongs to a fixed orbit of the natural action of G on the set $X \times X$. A well-known result by D.G. Higman asserts that G is primitive if and only if all the orbital graphs are connected. For a primitive group G , we define the *orbital diameter* of G to be the maximum of the diameters of all orbital graphs of G . Let $\mathcal{C}$ be an infinite class of finite primitive permutation groups. This gives rise to an infinite family of orbital graphs. It may be that the diameters of these orbital graphs tend to infinity. More interestingly, it may be that the diameters of all the orbital graphs are bounded above by some fixed constant; if this is the case, then we say that $\mathcal{C}$ is *bounded*. Previous results by M. W. Liebeck, D. Macpherson and K. Tent focus attention on classes of *almost simple* primitive permutation groups which are bounded.

In the thesis we analyse the orbital diameters of three families of groups, as follows. Firstly, we analyse the alternating and symmetric groups. For the primitive actions of these groups, we give necessary numerical conditions for the orbital diameter to be bounded above by some constant c and we make the result precise for $c = 5$. For each primitive action, we also describe either all or an infinite family of orbital graphs of diameter 2.

Then we analyse the almost simple groups with *socle* isomorphic to the *projective special linear group* $\mathrm{PSL}_2(q)$. For the primitive actions of these groups we give necessary conditions for the orbital diameter to be bounded above by 2 and we also give information about orbital graphs of diameter 2.

Lastly, we analyse a large family of simple groups known as the *simple groups of Lie type* which consist of the *simple classical groups* and *exceptional groups*. In particular, we analyse a class of primitive actions known as *parabolic actions*, giving a precise description of the actions for which the orbital diameter is at most 2. For the simple classical groups, we also describe infinite families of orbital graphs of diameter 2.

Contents

1	Introduction	11
1.1	Fundamental concepts	11
1.2	Motivation	14
2	Preliminary theory	21
2.1	Permutation groups	21
2.2	Bounds on diameters of orbital graphs	25
2.3	Classical groups	27
3	The alternating groups	34
3.1	Preliminary theory	35
3.2	Statements of the main results	36
3.3	Action of S_n on $I^{\{k\}}$	46
3.4	Action of S_n on $I^{(k,l)}$	60
3.5	Action of $G := S_n$ and A_n on $(G : H)$, where H is primitive . .	79
4	The projective special linear groups of dimension 2	84
4.1	Preliminary theory	84
4.2	Statement of the main result	89
4.3	$H \cap S \cong D_{q \pm 1}$	92
4.4	$H \cap S \cong \text{PGL}_2(q^{1/2})$	117
4.5	$H \cap S \cong \text{PSL}_2(q^{1/t})$	126

4.6	$H \cap S \cong A_4, A_5, S_4$	130
4.7	Proof of the main result	134
5	Computations using Magma	136
5.1	$C_{\text{DIAM}}^G(k, l)$, $G = S_n$	136
5.2	$C_{\text{DIAM}}^G(k, l)$, $G = A_n$	144
5.3	$C_{\text{LOW}}(k, l, \sigma)$	145
5.4	$C_{\text{VAL}}^G(d, L)$	146
5.5	$C_{\text{LOW}}^G(d, L)$	147
5.6	$C_{\text{DIAM}}^G(d, L)$	149
5.7	$C_{\text{LOW}}^{G,H}(d, L)$	150
5.8	$C_{\text{DIAM}}^{G,H}(q)$	154
5.9	$C_{\text{DIAM}}^{\text{PSL}_2}(q)$	154
5.10	$C_{\text{D}\pm}^{\text{PSL}_2}(q)$	155
5.11	$C_{\text{DIAM}}^{\text{PGL}_2}(q)$	156
6	Parabolic actions of the simple groups of Lie type	158
6.1	Preliminary theory	158
6.2	Statements of the main results	161
6.3	Maximal parabolic subgroups of the simple classical groups . .	163
6.4	Orbital graphs of the parabolic actions of the simple classical groups	166
6.5	Proof of the main result for the simple classical groups	174
6.6	Proof of the main result for the exceptional groups of Lie type	181
7	Open problems	184
Appendices		
A	Number theoretical methods	189

List of Tables

1.1	L -ranks of the alternating groups and groups of Lie type . . .	15
3.1	Pairs (k, l) with $\text{diam}_O(G, I^{(k,l)}) \leq 5$	42
3.2	Pairs (n, H) with $\text{diam}_O(S_n, \Omega) \leq 5$, where $\Omega := (S_n : H)$ and H is primitive	43
3.3	Pairs (n, H) with $\text{diam}_O(A_n, \Omega) \leq 5$, where $\Omega := (A_n : H)$ and H is primitive	43
3.4	Pairs (n, H) such that (S_n, Ω) has an orbital graph of diameter 2, where $\Omega := (S_n : H)$ and H is primitive	45
3.5	Pairs (n, H) such that (A_n, Ω) has an orbital graph of diameter 2, where $\Omega := (A_n : H)$ and H is primitive	45
3.6	Criterion for distance $v = 2r$ in the graph $\Gamma_{n,k,i}$, where $r \geq 2$.	49
3.7	Criterion for distance $v = 2r + 1$ in the graph $\Gamma_{n,k,i}$, where $r \geq 1$	50
3.8	Possible pairs (k, l) with $\text{diam}_O(G, I^{(k,l)}) \leq 5$	64
3.9	Possible pairs (n, H) with $\text{diam}_O(S_n, \Omega) \leq 5$, where $\Omega := (S_n : H)$ and H is primitive	80
3.10	Possible pairs (n, H) with $\text{diam}_O(A_n, \Omega) \leq 5$, where $\Omega := (A_n : H)$ and H is primitive	81
4.1	Maximal subgroups of G , where $\text{soc}(G) \cong \text{PSL}_2(q)$ and q is odd	88
4.2	Diameters of orbital graphs of (G, X) , where $\text{soc}(G) \cong \text{PSL}_2(q)$ and $q \leq 13$ is odd	91
4.3	Suborbits of $(\text{SO}_3(q), X_s)$	102

4.4	Suborbits of $(\Omega_3(q), X_s)$, where $q \equiv 1 \pmod{4}$	102
4.5	Suborbits of $(\Omega_3(q), X_s)$, where $q \equiv 3 \pmod{4}$	103
4.6	Suborbits of $(\text{SO}_3(q), X_n)$	109
4.7	$\text{diam}_O(G, X) \leq c \Rightarrow q < \epsilon m^{\frac{10c}{29}}$, where $X := (G : H)$	130
4.8	Pairs (G, X) with $\text{diam}_O(G, X) \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$	131
4.9	Orbital graphs of diameter 2 for (G, X) , where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$	131
4.10	Possible pairs (G, X) with orbital graph of diameter $c \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$	132
4.11	Possible pairs (G, X) with $\text{diam}_O(G, X) \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$	133
6.1	Pairs (X_n, k) ($k \neq 1$) such that $\text{diam}_O(G, Y) \leq 2$, where $G := \text{PX}_n(q)$ and $Y := (G : P_k)$	162
6.2	Diameter of a special orbital graph of (G, P_k)	180

Notation

Let G and H be groups, Ω a set, n a positive integer and q a prime power. We will use the following notation throughout this text.

C_n	Cyclic group of order n
D_n	Dihedral group of order n
S_n	Symmetric group of degree n
A_n	Alternating group of degree n
1_G	The identity element in G
$(G : H)$	The set of right cosets of H in G
$H <_{\max} G$	H is a maximal subgroup of G
$N_G(H)$	The normaliser of H in G
$G = N.Q$ (or $n.Q$)	Extension of N (or C_n) by Q , i.e. $G/N \cong Q$
$\mathbb{F}_q$	Field of q elements
$\mathbb{F}_q^*$	Non-zero elements of the field $\mathbb{F}_q$
I_n	$n \times n$ identity matrix
M^T	Transpose of the matrix M
δ_{ij}	Kronecker delta
X^n	The set of n -tuples with entries in X
C	Appears as the first letter of any computer program
$\text{diam}_O(G, \Omega)$	The orbital diameter of the permutation group (G, Ω)

Chapter 1

Introduction

1.1 Fundamental concepts

Throughout this text, a permutation group will be denoted by a pair (G, X) , where G is a group with a right action on a set X . For $x, y \in X$, the stabiliser in G of x will be denoted by G_x , and the stabiliser in G of x and y will be denoted by G_{xy} . If the cardinality of X is finite, then (G, X) is called finite. All permutation groups in this text will be assumed finite.

Let n be a positive integer. Recall that a permutation group (G, X) is called *n-transitive* if for any two n -tuples $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$ each consisting of n distinct elements of X , there exists $g \in G$ such that $\alpha_i^g = \beta_i$ for all i . We say that (G, X) is *transitive* if it is 1-transitive. A transitive permutation group (G, X) is called *primitive* if there is no non-trivial equivalence relation on X which is preserved by G .

The main objects of focus in the thesis will be a certain class of graphs called *orbital graphs*, which we now define.

Definition 1.1.1. Let (G, X) be a transitive permutation group.

1. An *orbital* of (G, X) is an orbit of the natural action of G on X^2 . The number of orbitals is called the *rank* of (G, X) . The *diagonal orbital* is

the orbital

$$\Delta_0 := \{(x, x) : x \in X\}.$$

2. For a non-diagonal orbital Δ , the *orbital graph* of Δ is the undirected graph with vertex set X and edges $\{x, y\}$ where $(x, y) \in \Delta$.

The orbital graphs of a primitive permutation group are all connected; the following well-known result justifies this.

Proposition 1.1.2. *Let (G, X) be a transitive permutation group where $|X| \geq 2$. The following are equivalent:*

1. (G, X) is primitive;
2. The point stabiliser G_x is a maximal subgroup of G , for all $x \in X$;
3. All the orbital graphs of (G, X) are connected.

Proof. The implication $(1) \Leftrightarrow (2)$ can be found as Corollary 1.5A in [9], and the implication $(1) \Leftrightarrow (3)$ can be found as Theorem 3.2A in [9]. $\square$

Since the orbital graphs of a primitive permutation group are all connected, we can define a quantity called the *orbital diameter* of the permutation group as follows.

Definition 1.1.3. Let (G, X) be a primitive permutation group and Γ be an orbital graph of (G, X) .

1. For two vertices $a \neq b$ of Γ , the *distance* between a and b is the length of a shortest path between a and b .
2. The *diameter* of Γ is the maximum of the distances between a and b over all pairs of vertices $a \neq b$ of Γ .
3. The *orbital diameter* of (G, X) is defined to be the maximum of the diameters of all orbital graphs of (G, X) , and is denoted by $\text{diam}_O(G, X)$.

In the thesis we will be focusing on the orbital diameters of particular types of primitive permutation groups, namely *almost simple* primitive permutation groups; we now define these.

For a group G , we will denote by $\text{Aut}(G)$ the group of all automorphisms of G , and we will denote by $\text{Inn}(G)$ the (normal) subgroup of $\text{Aut}(G)$ consisting of inner automorphisms of G , i.e. the automorphisms of G which are conjugation by elements of G . We will denote by $\text{Out}(G)$ the quotient group $\text{Aut}(G)/\text{Inn}(G)$. It is an easy to prove fact that $\text{Inn}(G) \cong G$, for a non-abelian simple group G ; henceforth, in this case we will write G in place of $\text{Inn}(G)$ when it is convenient.

Definition 1.1.4. A group G is called *almost simple* if it satisfies

$$\text{Inn}(T) \leq G \leq \text{Aut}(T),$$

for some non-abelian simple group T .

Definition 1.1.5. Let G be a non-trivial group.

1. A *minimal normal subgroup* of G is a non-trivial normal subgroup of G which does not contain properly any other non-trivial normal subgroup of G .
2. The *socle* of G is the subgroup generated by all the minimal normal subgroups of G , and is denoted by $\text{soc}(G)$.

In the following, for a group G and subgroup H , we denote by $C_G(H)$, the centraliser of H in G , i.e. the set of elements of G which commute with every element of H .

Proposition 1.1.6. *Let T be a non-abelian simple group and let G be an almost simple group with $\text{Inn}(T) \leq G \leq \text{Aut}(T)$. Then $\text{soc}(G) = \text{Inn}(T)$.*

Proof. Firstly, since T is a non-abelian simple group we have $\text{Inn}(T) \cong T$, and thus $\text{Inn}(T)$ is a minimal normal subgroup of G ; we will show that it is

the unique one and thus equal to the socle of G . Now suppose $M \neq \text{Inn}(T)$ is another minimal normal subgroup of G . It is a fact that any two elements from different minimal normal subgroups commute with each other (see Theorem 4.3A(i) in [9]), and thus $M \subseteq C_G(\text{Inn}(T))$. We claim that $C_G(\text{Inn}(T)) = 1$, which would imply the contradiction that $M = 1$, and complete the proof. To prove the claim, let $g \in C_G(\text{Inn}(T))$ and let $x_t : T \rightarrow T$ denote the map which is conjugation by $t \in T$. Then $x_t = gx_tg^{-1} = x_{g(t)}$ for all $t \in T$, where the last equality is straightforward to show. Thus $g(t)$ and t induce the same inner automorphism of T . This implies $g(t)^{-1}t$ is in the centre of T , which is trivial as it is a proper normal subgroup of the non-abelian simple group T . Hence $g(t) = t$ for all $t \in T$, i.e. $g = 1$. This proves the claim. $\square$

1.2 Motivation

Let $\mathcal{C}$ be an infinite class of finite primitive permutation groups. This gives rise to an infinite family of orbital graphs. It may be that the diameters of these orbital graphs tend to infinity. More interestingly, it may be that the diameters of all the orbital graphs are bounded above by some fixed constant.

Definition 1.2.1. Let $\mathcal{C}$ be an infinite class of finite primitive permutation groups. We say that $\mathcal{C}$ is *bounded* if there exists a constant d such that the diameters of all the orbital graphs of groups in $\mathcal{C}$ are bounded above by d .

The motivation behind the main results in the thesis is a result by M.W. Liebeck, D. Macpherson and K. Tent which gives structural information about the infinite classes of finite primitive permutation groups which are bounded. The finite primitive permutation groups can be split into five categories by the O’Nan-Scott theorem [17]; one category amongst these is the category of almost simple primitive permutation groups. The main result by Liebeck, Macpherson and Tent deals with all five classes of primitive permutation groups (see Theorem 1.1 in [15]), however we will only state the result

concerning almost simple groups as these are the groups we focus on in the thesis. We now make some definitions which are needed to state the result.

We begin with the classification of the finite simple groups. For the following result, see Section 1.2 in [24]. In the result, we shall use terms which we have not yet defined; we shall define the terms which are necessary as the need arises.

Theorem 1.2.2. *Every finite simple group is isomorphic to one of the following groups:*

1. *a cyclic group of prime order;*
2. *an alternating group of degree at least 5;*
3. *a group of Lie type*
4. *one of 26 sporadic groups;*

In fact, the majority of the groups in Theorem 1.2.2 (except for finitely many cases) are simple.

The main theorem in [15] deals with two categories of almost simple primitive permutation groups. To define these categories we make the following definition; again we use undefined terms which shall be defined in later chapters if needed.

Definition 1.2.3. Let G be an almost simple group with socle G_0 . We define a quantity called the L -rank of G when G_0 is one of the groups in Table 1.1.

	G_0	L -rank
(A)	A_n	n
(B)	$\text{PSL}_n(q), \text{P}\Omega_{2n}^-(q)$	$n - 1$
(C)	$\text{PSU}_{2n}(q), \text{PSU}_{2n+1}(q), \text{PSp}_{2n}(q), \text{P}\Omega_{2n+1}(q), \text{P}\Omega_{2n}^+(q)$	n
(D)	$E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$	6, 7, 8, 4, 2
(E)	${}^3D_4(q), {}^2E_6(q), {}^2B_2(q), {}^2G_2(q), {}^2F_4(q)'$	4, 6, 2, 2, 4

Table 1.1: L -ranks of the alternating groups and groups of Lie type

Remark 1.2.4. The groups excluding A_n in Table 1.1, comprise the groups of *Lie type* which are defined with respect to a finite field $\mathbb{F}_q$; we will denote by $G(q)$ a group of Lie type. The groups of Lie type are simple excluding finitely many cases (see [24, p. 3] for the precise result); the simple ones are collectively referred to as the *simple groups of Lie type*. In particular, the groups in rows (B) and (C) which are simple are known collectively as the *simple classical groups*; roughly speaking these are quotients of subgroups of the special linear group $\mathrm{SL}_n(q)$ (with coefficients in $\mathbb{F}_q$) by their centres (see Chapter 2 for detailed definitions). The simple groups containing the symbol Ω will be referred to as the *simple orthogonal groups*. The groups in rows (D) and (E) will be referred to as the *exceptional groups (of Lie type)*. Note that the final three groups in row (E) are each defined with respect to a finite field $\mathbb{F}_q$ of a certain characteristic. In particular ${}^2F_4(q)'$ (which denotes the commutator subgroup of ${}^2F_4(q)$) is defined for $q = 2^{2n+1}$ ($n \geq 0$) and ${}^2F_4(2^{2n+1})' = {}^2F_4(2^{2n+1})$ for $n \geq 1$ since ${}^2F_4(2^{2n+1})$ is simple for $n \geq 1$ (see Section 1.2 in [24]).

Definition 1.2.5. Let $n \geq 1$ be an integer. The group $\mathrm{PSL}_n(q)$ is defined to be the quotient of the group $\mathrm{SL}_n(q)$ by its centre. The map $A \mapsto (A^{-1})^T$ for $A \in \mathrm{SL}_n(q)$, is called the *graph automorphism* of $\mathrm{SL}_n(q)$.

We now define some particular actions of almost simple groups; again we use undefined terms which shall be defined in later chapters if needed.

Definition 1.2.6. Let (G, X) be an almost simple finite primitive permutation group with socle G_0 , and let $t \geq 1$ be an integer. We say that (G, X) has a *standard t -action* if one of the following holds:

1. $G_0 = A_n$ and X is the set of t -subsets of $\{1, \dots, n\}$ with the natural action of A_n ;
2. G_0 is a simple classical group (acting naturally on the subspaces of the underlying vector space V) and X is an orbit of subspaces of dimension

or codimension t ; the subspaces are arbitrary if $G_0 = \text{PSL}_n(q)$, and are otherwise *totally singular*, *non-degenerate*, or, if G_0 is a simple orthogonal group in characteristic 2, are *non-singular* subspaces of dimension 1 (in which case $t = 1$);

3. $G_0 = \text{PSL}_n(q)$, G contains an element from the coset in $\text{Out}(G_0)$ of the graph automorphism, and X is an orbit of pairs of subspaces $\{U, W\}$ of the underlying vector space V , where either $U \subseteq W$ or $V = U \oplus W$, and U has dimension t and W has dimension $n - t$;
4. $G_0 = \text{PSp}_{2n}(q)$, q is even, and the stabiliser in G_0 of a point is isomorphic to $\text{PO}_{2n}^\pm(q)$ (here we take $t = 1$).

We make one final definition before we state the main result by Liebeck, Macpherson and Tent.

Definition 1.2.7. Let $G := G(q)$ be a group of Lie type. A *subfield subgroup* of G is defined to be a group $N_G(G(q_0))$, where $G(q_0)$ is embedded naturally in G and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$.

Theorem 1.2.8 (Theorem 1.1(2) and (3) in [15]). *Let $\mathcal{C}$ be an infinite class of almost simple finite primitive permutation groups whose socle is either an alternating group or a group of Lie type, and suppose that $\mathcal{C}$ is bounded (say all the orbital diameters are bounded above by d). The following hold:*

1. *If the groups in $\mathcal{C}$ have unbounded L -ranks, then the socles of groups of sufficiently large L -rank are alternating or simple classical groups in standard t -actions, where t is bounded (in terms of d);*
2. *If the groups G in $\mathcal{C}$ have bounded L -rank, then the point stabilisers G_x have unbounded orders; moreover, if G has socle $G(q)$ of Lie type and G_x is a subfield subgroup $N_G(G(q_0))$, then $|\mathbb{F}_q : \mathbb{F}_{q_0}|$ is bounded (in terms of d).*

In fact the converse of Theorem 1.2.8 also holds (see Proposition 4.1(ii) and Theorem 1.2 in [15]). It can be seen that Theorem 1.2.8 gives structural information about classes of primitive permutation groups that are bounded, however it doesn't give explicit descriptions of classes for which the orbital diameters are bounded above by a given constant d . This brings us to the two broad aims of the thesis, which are as follows:

1. Given a constant d , to find all the almost simple finite primitive permutation groups (G, X) with $\text{diam}_O(G, X) \leq d$;
2. To find all the almost simple finite primitive permutation groups for which there exists an orbital graph of diameter d , for small values of d .

Note that aim 1 also involves analysing infinite classes of primitive permutation groups which are not bounded; a class which is not bounded can give rise to finitely many permutation groups whose orbital diameters are bounded above by a fixed constant. The motivation behind the second aim is the fact that orbital graphs belong to a wider, extensively studied family of graphs, namely *edge-transitive* graphs (a graph Γ is called edge-transitive if for any two edges e_1 and e_2 of Γ , there exists an automorphism of Γ that maps e_1 to e_2). Thus finding families of orbital graphs of small diameter amounts to producing edge-transitive graphs of small diameter.

In the thesis, we work on aims 1 and 2 for some values of $d \leq 5$, with almost simple groups whose socle is either an alternating group or a group of Lie type. Let us discuss what Theorem 1.2.8 tells us in each case. Let $\mathcal{C}$ be an infinite class of finite primitive permutation groups (G, X) .

Firstly, we analyse the case where $G := S_n$ or A_n for $n \geq 5$; it is a well-known that for $n \neq 6$, $\text{Aut}(A_n) \cong S_n$ (see Theorem 2.3 in [24]) and thus S_n and A_n are the only almost simple groups with socle equal to A_n . We shall see later that there are three different types of primitive actions of G ; Theorem 1.2.8(1) and its converse tells us that if we let n tend to infinity, then the only primitive action of G which will give rise to a bounded

class, is the action on t -subsets of $\{1, \dots, n\}$ where t is bounded. For the remaining two types of actions, we find necessary numerical conditions for the orbital diameter to be bounded above by some constant c , and give precise descriptions of the actions for which the orbital diameters are bounded by 5. For each primitive action, we also either determine all orbital graphs of diameter 2 or give descriptions of infinite families of orbital graphs of diameter 2. In fact, for the action of G on t -subsets, we give explicit formulas for the diameters of all orbital graphs. The main results of the chapter are Theorems 3.2.5, 3.2.6 and 3.2.8.

Secondly, we analyse almost simple groups G where $\text{soc}(G) \cong \text{PSL}_2(q)$ and q is odd. In this case we shall see that there are eight different types of primitive actions; Theorem 1.2.8(2) and its converse tells us that if we let q tend to infinity then four of these will give rise to bounded classes and the other four will not. In the thesis, we find the possible primitive actions of G for which the orbital diameter is at most 2 and also give descriptions of orbital graphs of diameter 2. The main result of the chapter is Theorem 4.2.1.

Lastly, we analyse the simple groups of Lie type which form a large proportion of the finite simple groups (see Theorem 1.2.2); we analyse a particular class of primitive actions known as the *parabolic actions*. For the simple classical groups, we shall see later that the parabolic actions are standard t -actions for some t , and thus Theorem 1.2.8(1) and its converse tells us that if we let the L -rank tend to infinity then this will give rise to a bounded class provided that t is bounded. In the thesis, we find the parabolic actions of the simple classical groups for which the orbital diameter is at most 2 and also give descriptions of orbital graphs of diameter 2; the main result is Theorem 6.2.1. For the exceptional groups, the stabilisers of the parabolic actions have unbounded orders as q tends to infinity (see Chapter 4 in [24] for the orders) and thus by Theorem 1.2.8, this case also gives rise to a bounded class. In the thesis, we find the parabolic actions of the exceptional groups for which the orbital diameter is at most 2; the main result is Theorem 6.2.5.

The structure of the thesis is as follows. We start by gathering together some preliminary material which is needed throughout the thesis in Chapter 2. In Chapter 3 we analyse the orbital diameters of primitive actions of the alternating and symmetric groups. In Chapter 4 we analyse the orbital diameters of primitive permutation groups whose socle is the group $\text{PSL}_2(q)$ where q is odd. The proofs of some of the results in Chapters 3 and 4 involve computations done using a computer; we explain the computer programs that we have written for these computations in Chapter 5. In Chapter 6, we analyse the orbital diameters of the parabolic actions of the simple groups of Lie type. We conclude the thesis with Chapter 7 which has a brief discussion of possible open problems which arise from the work done in the thesis.

Chapter 2

Preliminary theory

In this chapter we detail the preliminary theory which will be needed throughout the thesis.

2.1 Permutation groups

For a permutation group (G, X) , the orbit of $x \in X$ under G will be denoted by x^G and the action of $g \in G$ on $x \in X$ will be denoted by x^g . We recall a few definitions below.

Definition 2.1.1. Let (G, X) be a transitive permutation group.

1. An orbital of (G, X) is an orbit of the natural action of G on X^2 . The number of orbitals is called the rank of (G, X) . The diagonal orbital is the orbital

$$\Delta_0 := \{(x, x) : x \in X\}.$$

2. For an orbital Δ , we define the *paired* orbital

$$\Delta^* := \{(y, x) \in X^2 : (x, y) \in \Delta\}.$$

If $\Delta = \Delta^*$, then we say that Δ is *self-paired*.

3. For a non-diagonal orbital Δ , the orbital graph of Δ is the undirected graph with vertex set X and edges $\{x, y\}$ where $(x, y) \in \Delta$.
4. If (G, X) is primitive, then the orbital diameter of (G, X) is the maximum of the diameters of all orbital graphs of (G, X) , and is denoted by $\text{diam}_O(G, X)$.
5. Fix $x \in X$. A *suborbit* of (G, X) (with respect to x) is an orbit of G_x on X . The *trivial* suborbit is $\{x\}$.

Remark 2.1.2.

1. It is straightforward to see that a permutation group (G, X) which has rank equal to 2 has only one orbital graph of diameter 1 and hence has orbital diameter equal to 1. Similarly, a permutation group which has rank equal to 3 has either only one orbital graph of diameter 1 or two orbital graphs both of diameter 2, and hence in this case the orbital diameter is either 1 or 2, respectively.
2. We will use the notation $d_\Gamma(\alpha, \beta)$ to denote the distance between two vertices $\alpha \neq \beta$ of a graph Γ , and we will omit Γ from the notation if the graph in question is clear. If $d(\alpha, \beta) = 1$, i.e. $\{\alpha, \beta\}$ is an edge, then we may write $\alpha - \beta$. When computing the diameter of an orbital graph of a primitive permutation group (G, X) , it is useful to note that since G acts transitively on each orbital, if (α, β) and (γ, δ) are in the same orbital, then $d(\alpha, \beta) = d(\gamma, \delta)$.

When analysing the orbitals of a transitive permutation group, we will often use the well-known correspondence between orbitals and suborbits which can be found in [9, p. 67] and is as follows.

Proposition 2.1.3. *Let (G, X) be a transitive permutation group and let $x \in X$. There is a one-to-one correspondence between orbitals of (G, X) and suborbits of (G, X) , where the suborbit y^{G_x} corresponds to the orbital $(x, y)^G$ and an orbital Δ corresponds to the suborbit $\Delta(x) := \{y \in X : (x, y) \in \Delta\}$.*

In light of Proposition 2.1.3, we say that a suborbit is self-paired if the corresponding orbital is self-paired.

In various chapters of the thesis, we will need to work out the sizes of stabilisers of points in certain actions, or justify that a particular permutation group is transitive; we do these using the following well-known result.

Proposition 2.1.4 (Orbit-Stabiliser property, [9, Theorem 1.4A(iii)]). *Let (G, X) be a permutation group. Then $|x^G| = |G : G_x|$ for all $x \in X$. Thus if $|G : G_x| = |X|$, then (G, X) is transitive.*

When analysing the primitive actions of a group, we will sometimes also need to analyse the restriction of the action to a subgroup of index 2. For this purpose we state and prove the following result.

Proposition 2.1.5. *Let (G, X) and (H, X) be transitive permutation groups. Suppose $H \leq G$ is a subgroup of index 2. Let $\Delta := y^{G_x}$ be a non-trivial suborbit of (G, X) . Then either $|G_{xy} : G_{xy} \cap H| = 1$, in which case Δ splits into 2 suborbits of (H, X) of equal size, or $|G_{xy} : G_{xy} \cap H| = 2$, in which case Δ remains a suborbit of (H, X) .*

Proof. Firstly note that using the Orbit-Stabiliser property we have

$$|G_x \cap H| = |H_x| = |G_x|/2. \quad (2.1)$$

Secondly note that

$$|G_{xy} : G_{xy} \cap H| = \frac{|G_{xy}|}{|G_{xy} \cap H|} = \frac{|G_{xy}H|}{|H|} \leq \frac{|G|}{|H|} = 2.$$

Suppose $|G_{xy} : G_{xy} \cap H| = 1$. Then $G_{xy} = G_{xy} \cap H$ and hence using the Orbit-Stabiliser property and (2.1) we obtain

$$|y^{H_x}| = |y^{G_x \cap H}| = |G_x \cap H : G_{xy}| = \frac{|G_x|}{2|G_{xy}|} = \frac{|\Delta|}{2},$$

i.e. Δ splits into two suborbits of (H, X) of equal size. Now suppose $|G_{xy} : G_{xy} \cap H| = 2$. Then again using the Orbit-Stabiliser property and (2.1) we obtain

$$|y^{H_x}| = |y^{G_x \cap H}| = |G_x \cap H : G_{xy} \cap H| = \frac{|G_x|}{|G_{xy}|} = |\Delta|,$$

i.e. Δ is a suborbit of (H, X) . $\square$

Remark 2.1.6. Let (G, X) and (H, X) be as in Proposition 2.1.5, and let $\Delta := (\alpha, \beta)^G$ be an orbital of (G, X) . Then $|\Delta| = |G : G_{(\alpha, \beta)}| = |X||\beta^{G_\alpha}|$. Thus, Δ splits into 2 orbitals of (H, X) if and only if the corresponding suborbit β^{G_α} does.

There are certain classes of primitive permutation groups for which the sets of diameters of all orbital graphs are equal, and therefore to study the orbital diameters of these permutation groups, it would suffice to analyse the most convenient permutation group out of the class. Below we make this notion more precise.

Definition 2.1.7. Let (G, X) and (H, Y) be two permutation groups. We say that (G, X) and (H, Y) are *(permutation) isomorphic* if there exists an isomorphism $\phi : G \rightarrow H$ and a bijection $f : X \rightarrow Y$ such that

$$f(x^g) = f(x)^{\phi(g)}, \quad \forall x \in X, g \in G.$$

If $G = H$ and $\phi = 1_G$, then we say that (G, X) and (H, Y) are *(permutation) equivalent*.

We now state a result summarising some facts which are either straightforward to prove or can be found in an introductory text on permutation groups such as [9].

Proposition 2.1.8.

1. *Every primitive action of a group G on a set X is equivalent to the natural action (of right multiplication) of G on the set $(G : H)$ of right cosets of H in G , where $H := G_\alpha$ ($\alpha \in X$) is a maximal subgroup of G .*
2. *For a group G and subgroups H and K , the natural transitive actions of G on $(G : H)$ and $(G : K)$ are equivalent if and only if H and K are conjugate in G .*
3. *The set of diameters of all orbital graphs of a primitive permutation group is preserved under permutation isomorphisms.*

To summarise, Proposition 2.1.8 justifies the following: in order to study the orbital diameters of the primitive actions of a group G , it suffices to study the natural actions of G on right cosets of conjugacy class representatives of maximal subgroups of G .

2.2 Bounds on diameters of orbital graphs

In this section we state and prove two results which are bounds involving the diameter of an orbital graph. These results will be used in various chapters to narrow down possibilities for permutation groups whose orbital diameters are bounded above by some fixed constant.

Lemma 2.2.1. *Let (G, X) be a primitive permutation group where $X := (G : H)$ and $|H| > 1$. Let Γ be an orbital graph of (G, X) with diameter d . Then Γ is regular of valency $k \leq 2|H|$ and*

$$|G : H| \leq 1 + 2|H| + 2|H|(2|H| - 1) + \cdots + 2|H|(2|H| - 1)^{d-1} \quad (2.2)$$

$$< \frac{|H|}{|H| - 1} (2|H| - 1)^d. \quad (2.3)$$

Proof. The regularity of Γ follows from the transitivity of G on X . Let $\Delta := (\alpha, \beta)^G$ be the orbital corresponding to Γ . Recall that the vertex set of Γ is X . Let k be the valency of $\alpha \in X$. We have $(\gamma, \alpha) \in \Delta$ for some γ . Then $\{\alpha, \delta\}$ is an edge if and only if $\delta \in \beta^{G_\alpha}$ or $\delta \in \gamma^{G_\alpha}$. Now these two suborbits are equal if and only if Δ is self-paired, therefore either $k = |\beta^{G_\alpha}|$ or $k = |\beta^{G_\alpha}| + |\gamma^{G_\alpha}|$. In either case, $k \leq |\beta^{G_\alpha}| + |\gamma^{G_\alpha}| \leq 2|G_\alpha| = 2|H|$. This proves the upper bound on the valency. To prove the last assertion observe that,

$$|X| \leq 1 + k + k(k-1) + \cdots + k(k-1)^{d-1}.$$

Now $k \leq 2|H|$ and using this in the above inequality we obtain

$$\begin{aligned} |G : H| &\leq 1 + 2|H| + 2|H|(2|H| - 1) + \cdots + 2|H|(2|H| - 1)^{d-1} \\ &= 1 + 2|H| \left(\frac{(2|H| - 1)^d - 1}{2|H| - 2} \right) \\ &< \frac{|H|}{|H| - 1} (2|H| - 1)^d. \end{aligned}$$

□

Proposition 2.2.2. *Let (G, X) be a primitive permutation group where $X := (G : H)$. Suppose there exists a subgroup $Y \leq H$ such that $N_G(Y) > N_H(Y)$. If $N_G(Y) \setminus N_H(Y)$ contains an element of order 2, then define $a := 1$, otherwise define $a := 2$. There exists an orbital graph of diameter d , where*

$$d > \frac{\log(|X|)}{\log(a|H|) - \log(|Y|)} - 1.$$

Proof. Pick $g \in N_G(Y) \setminus N_H(Y)$. Define $\alpha := H$, $\beta := Hg$, and $k := |\beta^{G_\alpha}|$. Let Γ be the orbital graph corresponding to the orbital $\Delta := (\alpha, \beta)^G$ and define $d := \text{diam}(\Gamma)$. If g has order 2, then g swaps α and β , and hence Δ is self-paired, i.e. Γ has valency k . Otherwise Γ has valency $2k$. By the proof

of Lemma 2.2.1 we have that

$$|G : H| \leq 1 + ak + ak(ak - 1) + \cdots + ak(ak - 1)^{d-1} < (ak)^{d+1},$$

where a is as in the statement of the lemma. Rearranging for d , this implies

$$d > \frac{\log(|G : H|)}{\log(ak)} - 1. \quad (2.4)$$

By the Orbit-Stabiliser property, we have $k = |G_\alpha : G_{\alpha\beta}|$. Moreover, since $G_\beta = g^{-1}G_\alpha g$, we thus have $k = |G_\alpha : G_\alpha \cap g^{-1}G_\alpha g|$. Now $Y \leq H = G_\alpha$ and $Y = g^{-1}Yg \leq g^{-1}G_\alpha g$ imply $|Y| \leq |G_\alpha \cap g^{-1}G_\alpha g|$, and hence $k \leq |H|/|Y|$. Using this in (2.4), we obtain the result. $\square$

2.3 Classical groups

In this section, we define a family of groups known as the *classical groups*. These give rise to the *simple classical groups* which will be the main groups we study in Chapters 4 and 6.

Henceforth, all vector spaces mentioned will be over a finite field $\mathbb{F}_q$. We will denote by $\text{GL}(V)$, the *general linear group* of all invertible linear transformations of a vector space V , and by $\text{SL}(V)$, the *special linear group* of elements of $\text{GL}(V)$ with determinant 1. The classical groups are defined as particular subgroups of $\text{SL}(V)$ and they arise from various maps on V which we describe next.

Definition 2.3.1. Let V be a vector space.

1. A map $f : V \times V \rightarrow \mathbb{F}_q$ is called a
 - (a) *symplectic form* if it is alternating, bilinear, and $f(v, v) = 0$ for all $v \in V$;

- (b) *unitary form* if it is left-linear and $f(v, w) = \sigma(f(w, v))$, where $q = q_0^2$ and $\sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ given by $x \mapsto x^{q_0}$ is an automorphism of $\mathbb{F}_q$ of order 2.

2. A map $Q : V \rightarrow \mathbb{F}_q$ is called a *quadratic form* if

- (a) $Q(\lambda v) = \lambda^2 v$, for all $v \in V$ and $\lambda \in \mathbb{F}_q$, and
(b) the map $f : V \times V \rightarrow \mathbb{F}_q$ defined by

$$f(v, w) := Q(v + w) - Q(v) - Q(w)$$

is bilinear.

In cases 1a and 1b, we refer to (V, f) as a *symplectic space* or *unitary space*, respectively, and in case 2, we refer to (V, Q) as a *quadratic space*.

Remark 2.3.2. Let $Q : V \rightarrow \mathbb{F}_q$ be a quadratic form and let f be the corresponding bilinear form. Then Q determines f but the converse only holds if q is odd.

Henceforth, for the maps f as in Definition 2.3.1, we will write (v, w) instead of $f(v, w)$.

Definition 2.3.3. Let V be a vector space and let $f : V \times V \rightarrow \mathbb{F}_q$ be a symplectic or unitary form, or the symmetric bilinear form associated to a quadratic form.

1. For a subspace $W \subseteq V$, define

$$W^\perp := \{v \in V : (v, w) = 0, \quad \forall w \in W\}.$$

2. We say that V (or the form) is *non-degenerate* if $V^\perp = 0$.
3. We say that a subspace $W \subseteq V$ is non-degenerate if $W \cap W^\perp = 0$.

Remark 2.3.4. Let V and W be as in Definition 2.3.3. If W is non-degenerate and $V = W + W^\perp$, we write $V = W \perp W^\perp$. We have that W is non-degenerate if and only if $V = W \perp W^\perp$ (see Lemma 2.1.5(v) in [14]).

We will need the following definition before we can define the *classical groups*. Henceforth, we will use the term (V, κ) to collectively denote the structures (V, f) and (V, Q) appearing in Definition 2.3.1, where $\kappa : V^l \rightarrow \mathbb{F}_q$ and $l := 1$ if (V, Q) is a quadratic space, and $l := 2$ if (V, f) is a symplectic or unitary space. Furthermore, we will omit the use of κ when it is clear from the context what κ is.

Definition 2.3.5. Let (V, κ) be a non-degenerate symplectic, unitary or quadratic space. We define

$$I(V, \kappa) := \{g \in \mathrm{GL}(V) : \kappa(g(\mathbf{v})) = \kappa(\mathbf{v}), \quad \forall \mathbf{v} \in V^l\},$$

and

$$S(V, \kappa) := \mathrm{SL}(V) \cap I(V, \kappa).$$

We say that $I(V, \kappa)$ *stabilises* κ .

Definition 2.3.6. The *classical groups* consist of the following groups:

- *Linear groups:* These are the groups $\mathrm{GL}(V)$ and $\mathrm{SL}(V)$;
- *Symplectic groups:* These are the groups $\mathrm{Sp}(V) := I(V, f)$, where (V, f) is a non-degenerate symplectic space;
- *Unitary groups:* These are the groups $\mathrm{U}(V) := I(V, f)$ and $\mathrm{SU}(V) := S(V, f)$, where (V, f) is a non-degenerate unitary space;
- *Orthogonal groups:* These are the groups $\mathrm{O}(V) := I(V, Q)$ and $\mathrm{SO}(V) := S(V, Q)$, where (V, Q) is a non-degenerate quadratic space, and the commutator subgroup of $\mathrm{SO}(V)$, denoted $\Omega(V)$.

When analysing actions of the classical groups, it will not be necessary to consider each possibility for (V, κ) separately. To explain precisely which (V, κ) we need to consider, we make the following definition and remark.

Definition 2.3.7. Let (V, κ) and (V', κ') be two spaces of the same dimension, which are both symplectic, both unitary or both quadratic.

1. An *isometry* is a linear map $g : V \rightarrow V'$ such that

$$\kappa'(g(\mathbf{v})) = \kappa(\mathbf{v}), \quad \forall \mathbf{v} \in V.$$

If the above holds, then we say that (V, κ) and (V', κ') are *isometric*.

2. A *similarity* is a linear map $g : V \rightarrow V'$ such that

$$\kappa'(g(\mathbf{v})) = \lambda \kappa(\mathbf{v}), \quad \forall \mathbf{v} \in V,$$

for some $\lambda \in \mathbb{F}_q$. If the above holds, then we say that (V, κ) and (V', κ') are *similar*.

Remark 2.3.8. If (V, κ) and (V', κ') are isometric or similar, and $I := I(V, \kappa)$ and $I' := I(V', \kappa')$, then there exists an $\mathbb{F}_q$ -linear homomorphism $g : V \rightarrow V'$ such that $gIg^{-1} = I'$, and hence there is a one-to-one correspondence between the actions of I and I' , where the corresponding actions are permutation isomorphic. Also note that a form κ on a vector space V is determined by the values it takes on a basis of V ; in the case where $V = V'$, by the above, it does not matter which values are chosen as long as all sets of values determine isometric or similar forms.

We now detail the number of isometry and similarity classes of non-degenerate symplectic, unitary and orthogonal spaces.

Proposition 2.3.9. (*Proposition 2.4.1 in [14]*). Let (V, f) be a non-degenerate symplectic space. Then the dimension n of V is even ($n = 2m$) and (V, f) is unique up to isometry. Furthermore, V has a basis $\{e_1, \dots, e_m, f_1, \dots, f_m\}$ such that

$$(e_i, e_j) = (f_i, f_j) = 0, \quad (e_i, f_j) = \delta_{ij}, \quad \forall i, j.$$

Proposition 2.3.10. (*Propositions 2.3.1 and 2.3.2 in [14]*). Let (V, f) be a non-degenerate unitary space. Then (V, f) is unique up to isometry. Furthermore, V has a basis

1. $\{e_1, \dots, e_m, f_1, \dots, f_m\}$, if $n = 2m$;
2. $\{e_1, \dots, e_m, f_1, \dots, f_m, x\}$, if $n = 2m + 1$,

where $(x, x) = 1$, and

$$(e_i, e_j) = (f_i, f_j) = 0, \quad (e_i, f_j) = \delta_{ij}, \quad (e_i, x) = (f_i, x) = 0, \quad \forall i, j.$$

Proposition 2.3.11. (*Propositions 2.5.3 and 2.5.4 in [14]*). For each n , there are precisely two isometry classes of non-degenerate quadratic spaces (V, Q) of dimension n . If n is odd, then all the spaces are similar. Furthermore, V has a basis of one of the following forms:

1. $\{e_1, \dots, e_m, f_1, \dots, f_m\}$ (with $n = 2m$), where

$$Q(e_i) = Q(f_i) = 0, \quad (e_i, f_j) = \delta_{ij}, \quad \forall i, j;$$

2. $\{e_1, \dots, e_{m-1}, f_1, \dots, f_{m-1}, x, y\}$ (with $n = 2m$), such that

$$Q(e_i) = Q(f_i) = 0, \quad (e_i, f_j) = \delta_{ij},$$

$$(e_i, x) = (e_i, y) = (f_i, x) = (f_i, y) = 0,$$

for all i, j , and $(Q(x), Q(y), (x, y)) = (1, \zeta, 1)$, where the polynomial $t^2 + t + \zeta$ is irreducible over $\mathbb{F}_q$;

3. $\{e_1, \dots, e_m, f_1, \dots, f_m, x\}$ (with $n = 2m + 1$), where

$$Q(e_i) = Q(f_i) = 0, \quad (e_i, f_j) = \delta_{ij}, \quad (e_i, x) = (f_i, x) = 0, \quad \forall i, j,$$

and $Q(x) \neq 0$.

The bases described in Propositions 2.3.9, 2.3.10 and 2.3.11 will be referred to as *standard bases*.

Definition 2.3.12. Let (V, Q) be a non-degenerate quadratic space. Let $W \subseteq V$ be a non-degenerate subspace and let Q_W denote the restriction of Q to W . We define

$$\operatorname{sgn}(Q) := \begin{cases} \circ, & \text{if } (V, Q) \text{ has a basis as in Proposition 2.3.11(3)} \\ +, & \text{if } (V, Q) \text{ has a basis as in Proposition 2.3.11(1)} \\ -, & \text{if } (V, Q) \text{ has a basis as in Proposition 2.3.11(2),} \end{cases}$$

and $\operatorname{sgn}(W) := \operatorname{sgn}(Q_W)$.

To distinguish between the orthogonal groups corresponding to the three different types of quadratic spaces (V, Q) in Proposition 2.3.11, we will write $Y^{\operatorname{sgn}(Q)}(V)$ instead of $Y(V)$ for $Y \in \{O, SO, \Omega\}$; if $\operatorname{sgn}(Q) = \circ$, we may omit the $\circ$. In order to determine $\operatorname{sgn}(Q)$ in later chapters, it will be helpful to define the following types of subspaces of V .

Definition 2.3.13. Let (V, Q) be a quadratic space. A subspace $W \leq V$ is called *totally singular* if $Q(w) = 0$ for all $w \in W$.

We conclude this chapter by defining the simple classical groups. It turns out that the classical groups themselves are not usually simple groups, but modulo their centres become simple in many cases.

Definition 2.3.14. Let $X \in \{GL, SL, Sp, U, SU, O, SO, O^\pm, SO^\pm, \Omega^\circ, \Omega^\pm\}$. The *projective* group $PX(V)$ is defined to be the group $X(V)/Z(X(V))$, where $Z(X(V))$ denotes the centre of $X(V)$.

Remark 2.3.15. Let V be a vector space of dimension n over $\mathbb{F}_q$. By fixing a basis of V we have that $\mathrm{GL}(V) \cong \mathrm{GL}_n(q)$. Under this isomorphism, the groups $X(V)$ for $X \in \{\mathrm{GL}, \mathrm{SL}, \mathrm{Sp}, \mathrm{U}, \mathrm{SU}, \mathrm{O}, \mathrm{SO}, \mathrm{O}^\pm, \mathrm{SO}^\pm, \Omega^\circ, \Omega^\pm\}$ will be denoted by $X_n(q)$. The corresponding projective groups will be denoted by $\mathrm{PX}_n(q)$. We will refer to n as the *dimension* of $X_n(q)$ and $\mathrm{PX}_n(q)$.

The following is a concatenation of Theorems 4.5, 8.8, 10.20 and 11.48 from [23].

Theorem 2.3.16. *Let $X \in \{\mathrm{SL}, \mathrm{Sp}, \mathrm{SU}, \Omega^\circ, \Omega^\pm\}$. The groups $\mathrm{PX}_n(q)$ are simple in the following cases:*

1. $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3)$, for $X = \mathrm{SL}$;
2. $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3), (4, 2)$, for $X = \mathrm{Sp}$;
3. $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3), (3, 2)$, for $X = \mathrm{SU}$;
4. $m \geq 1$ ($n = 2m + 1$) and $(n, q) \neq (3, 3)$, for $X = \Omega^\circ$;
5. $m \geq 3$ ($n = 2m$), for $X = \Omega^+$;
6. $m \geq 2$ ($n = 2m$), for $X = \Omega^-$.

The groups $\mathrm{PX}_n(q)$ in Theorem 2.3.16 will be referred to as the *simple classical groups*.

Chapter 3

The alternating groups

In this chapter we study the orbital diameters of the primitive actions of the symmetric and alternating groups S_n and A_n . We give necessary conditions for the orbital diameters to be bounded above by some constant c and give precise descriptions of the actions for which the orbital diameters are bounded above by 5. For each primitive action, we also either determine all orbital graphs of diameters 2 or give descriptions of infinite families of orbital graphs of diameter 2. Throughout the chapter we will assume that $n \geq 5$.

The chapter is split into five sections. We shall see later that the primitive actions of S_n and A_n can be analysed in three cases. In Section 3.1, we state the preliminary results we will need. In Section 3.2, we state the main results of the chapter, and in Sections 3.3, 3.4 and 3.5, we prove the main results by analysing the orbital graphs for each of the three cases of the primitive action of S_n and A_n .

The majority of the material in this chapter can be found in the form of a paper by the author in [21]. A few minor errors have been found in the paper after publication, which have been corrected in this chapter; the main error is in Theorem 1.3(2) in [21], which has been corrected in Theorem 3.2.8(2) of the chapter. Also, the notation for the graph Γ_i^n from [21] has been changed to $\Gamma_{n,k,i}$, and some text has been updated to improve readability.

3.1 Preliminary theory

In this section we present the background material which will be needed throughout the chapter.

Given groups G and H and a map $\phi : H \rightarrow \text{Aut}(G)$, we will denote by $G \rtimes_{\phi} H$, the semi-direct product of G and H with respect to ϕ . If the map ϕ is not specified, then we will write $G : H$. For groups A and B where B acts on the set $\{1, \dots, n\}$, we will denote by $A \wr B$, the wreath product of A and B , i.e. the semi-direct product $A^n \rtimes_{\phi} B$, where $\phi : B \rightarrow \text{Aut}(A^n)$ is given by $\phi(\pi) : (a_1, \dots, a_n) \mapsto (a_{1\pi^{-1}}, \dots, a_{n\pi^{-1}})$. Recall that in order to study the primitive actions of S_n and A_n , we need to know about their maximal subgroups. The following result splits the maximal subgroups of S_n and A_n into three classes.

Theorem 3.1.1. *If $H \neq A_n$ is a maximal subgroup of S_n , then one of the following holds:*

1. $H \cong S_k \times S_{n-k}$, where $1 \leq k < n/2$;
2. $H \cong S_k \wr S_l$, where $n = kl$ and $k > 1, l > 1$;
3. H is primitive on $\{1, \dots, n\}$.

Conversely, let H be as in (1) or (2). Then H is a maximal subgroup of S_n , and $H \cap A_n$ is a maximal subgroup of A_n provided $H \not\cong S_2 \wr S_4$.

Proof. If H is not transitive on $\{1, \dots, n\}$, then H fixes set-wise a set of size k for some $k \geq 1$, and thus $H \leq S_k \times S_{n-k}$. Since H is maximal in S_n , we have $H = S_k \times S_{n-k}$. Without loss of generality, we may suppose $k \leq n/2$ (if $k > n/2$, then $n - k < n/2$). Moreover, observe that $S_k \times S_k < S_k \wr S_2$, and thus H is not maximal if $n = 2k$. If H is transitive but not primitive on $\{1, \dots, n\}$, then $n = kl$, for some $k > 1, l > 1$ and H fixes a partition of $\{1, \dots, n\}$ into l sets each of size k . Thus $H \leq S_k \wr S_l$ and by the maximality of

H , we have $H = S_k \wr S_l$. In the remaining cases, H is primitive on $\{1, \dots, n\}$. For the converse, see the main theorem in [16]. $\square$

3.2 Statements of the main results

In order to state the main results, we will need to describe the orbital graphs of the primitive actions of S_n and A_n , and thus we begin by doing this.

Throughout this chapter I will denote the set $\{1, \dots, n\}$. We will denote by $I^{\{k\}}$ the set of k -subsets of I . If $n = kl$, then we will denote by $I^{(k,l)}$ the set of (k, l) -partitions of I (a (k, l) -partition of I is a partition of I into l sets, each of size k), and we will write $A = A_1 | \dots | A_l$ to mean that A is the (k, l) -partition of I into the l disjoint k -subsets A_i . For two (k, l) -partitions $A = A_1 | \dots | A_l$ and $B = B_1 | \dots | B_l$ of I , we will denote by I_{AB} the $l \times l$ matrix with entries $(I_{AB})_{ij} := |A_i \cap B_j|$. Note that the row and column sums of the matrix I_{AB} are k . Let $\mathcal{N}$ denote the set of all $l \times l$ matrices with non-negative integer entries, and row and column sums equal to k . Define an equivalence relation $\sim$ on $\mathcal{N}$, where $M \sim M'$ if and only if there exist permutation matrices P and Q such that $M' = PMQ$, i.e. M' can be obtained from M by a permutation of rows and columns. The equivalence class of $M \in \mathcal{N}$ will be denoted by $[M]$. The groups S_n and A_n act naturally on $I^{\{k\}}$ and $I^{(k,l)}$ and we now determine the orbitals of these actions.

Proposition 3.2.1. *Let $G := S_n$ and $1 \leq k \leq n/2$.*

1. *G acts transitively on $I^{\{k\}}$ and for $A \in I^{\{k\}}$, we have $G_A \cong S_k \times S_{n-k}$.*
2. *The non-diagonal orbitals of $(G, I^{\{k\}})$ are*

$$\Delta_{n,k,i} := \{(A, B) \in I^{\{k\}} \times I^{\{k\}} : |A \cap B| = i\}, \quad i \in \{0, \dots, k-1\}.$$

Proof. The transitivity is clear. Let $A \in I^{\{k\}}$ and let H and K be the subgroups of G_A fixing $I \setminus A$ and A pointwise, respectively. It is easy to see that

$G_A = \langle H, K \rangle$. Now $H \cong S_k$ and $K \cong S_{n-k}$, and H and K commute, hence $\langle H, K \rangle \cong S_k \times S_{n-k}$. This proves part 1. Clearly the sets $\Delta_{n,k,i}$ are non-empty, disjoint and their union (together with the diagonal orbital) is $I^{\{k\}} \times I^{\{k\}}$. Now suppose (A, B) and (C, D) are in the same orbital. Then there exists $g \in G$ such that $(C, D) = (A, B)^g$ and thus $|A \cap B| = |C \cap D|$. It remains to show that for a given i , G is transitive on $\Delta_{n,k,i}$. Indeed, given (A, B) and (C, D) in $\Delta_{n,k,i}$ with $A = \{a_1, \dots, a_k\}$, $B = \{a_1, \dots, a_i, a_{k+1}, \dots, a_{2k-i}\}$, $C = \{b_1, \dots, b_k\}$ and $D = \{b_1, \dots, b_i, b_{k+1}, \dots, b_{2k-i}\}$, any permutation mapping a_j to b_j for all j , is in G . This proves part 2. $\square$

Remark 3.2.2.

1. The proof of Theorem 3.1.1 asserts that every maximal subgroup of S_n which is not transitive is the stabiliser of a k -subset and thus by Proposition 3.2.1(1), for a fixed k , all such maximal subgroups are conjugate in S_n .
2. The natural action of $H := A_n$ on $I^{\{k\}}$ is transitive and for $A \in I^{\{k\}}$, we have $H_A = G_A \cap H$ where $G := S_n$. The orbitals of this action are again the sets $\Delta_{n,k,i}$ from Proposition 3.2.1. This follows from the fact that if (A, B) and (C, D) are in $\Delta_{n,k,i}$ and $g \in G$ such that $A^g = C$ and $B^g = D$, then either $g \in H$ or else g can be multiplied by a suitable transposition so that the resulting permutation h is in H and satisfies $A^h = C$ and $B^h = D$.
3. The orbital $\Delta_{n,k,i}$ from Proposition 3.2.1 is self-paired; the corresponding orbital graph will be denoted by $\Gamma_{n,k,i}$, and is the graph with vertex set $I^{\{k\}}$ and edges $\{A, B\}$ where $|A \cap B| = i$.
4. For $n > 2k$, the orbital graphs $\Gamma_{n,k,i}$ are connected. If $n = 2k$, then $\Gamma_{n,k,i}$ is connected for all $i \neq 0$. We will use results about the graphs $\Gamma_{2k,k,i}$ when analysing case 2 of Theorem 3.1.1; in all such results, we will assume $i \neq 0$.

Proposition 3.2.3. *Let $k, l > 1$, $n := kl$ and $G := S_n$.*

1. *G acts transitively on $I^{(k,l)}$ and for $A \in I^{(k,l)}$, we have $G_A \cong S_k \wr S_l$.*
2. *The orbitals of $(G, I^{(k,l)})$ are*

$$\Delta_{[M]} := \{(A, B) \in I^{(k,l)} \times I^{(k,l)} : I_{AB} \in [M]\}, \quad M \in \mathcal{N}.$$

Proof. The transitivity is clear. For $A \in I^{(k,l)}$, write $A = A_1 | \dots | A_l$. For $1 \leq i \leq l$, let $H_i \cong S_k$ be the subgroup of all permutations on $\{1, \dots, n\}$ which fix A_i setwise and fix A_j pointwise for $j \neq i$. Let K be the subgroup of all permutations on $\{1, \dots, n\}$ which permute the set of subscripts $\{1, \dots, l\}$. Then $G_A = \langle H_i, K : 1 \leq i \leq l \rangle \cong S_k \wr S_l$. This proves part 1. Now note that the sets $\Delta_{[M]}$ are non-empty; indeed given $M := (m_{ij}) \in \mathcal{N}$, the set $\Delta_{[M]}$ contains the pair of (k, l) -partitions (A, B) , where $A = A_1 | \dots | A_l$,

$B = B_1 | \dots | B_l$ and,

$$\begin{aligned}
A_1 &:= \{\overbrace{1, \dots, m_{11}}^{A_{11}}, \overbrace{m_{11} + 1, \dots, m_{11} + m_{12}}^{A_{12}}, \\
&\quad \vdots \\
&\quad \overbrace{m_{11} + \dots + m_{1l-1} + 1, \dots, m_{11} + \dots + m_{1l}}^{A_{1l}}\} \\
A_2 &:= \{\overbrace{m_{11} + \dots + m_{1l} + 1, \dots, m_{11} + \dots + m_{1l} + m_{21}}^{A_{21}}, \\
&\quad \overbrace{m_{11} + \dots + m_{1l} + m_{21} + 1, \dots, m_{11} + \dots + m_{1l} + m_{21} + m_{22}}^{A_{22}}, \\
&\quad \vdots \\
&\quad \overbrace{m_{11} + \dots + m_{1l} + m_{21} + \dots + m_{2,l-1} + 1,}^{A_{2l}} \\
&\quad \dots, m_{11} + \dots + m_{1l} + m_{21} + \dots + m_{2l}\} \\
&\quad \vdots \\
A_l &:= \{\overbrace{(m_{11} + \dots + m_{1l}) + \dots + (m_{l-1,1} + \dots + m_{l-1,l}) + 1, \dots,}^{A_{l1}} \\
&\quad (m_{11} + \dots + m_{1l}) + \dots + (m_{l-1,1} + \dots + m_{l-1,l}) + m_{l1}, \\
&\quad \vdots \\
&\quad \overbrace{(m_{11} + \dots + m_{1l}) + \dots + (m_{l-1,1} + \dots + m_{l-1,l}) + (m_{l1} + \dots + m_{l,l-1}) + 1,}^{A_{ll}} \\
&\quad \dots, (m_{11} + \dots + m_{1l}) + (m_{21} + \dots + m_{2l}) + \dots + (m_{l1} + \dots + m_{ll})\},
\end{aligned}$$

and,

$$\begin{aligned} B_1 &:= \{A_{11}, A_{21}, \dots, A_{l1}\} \\ B_2 &:= \{A_{12}, A_{22}, \dots, A_{l2}\} \\ &\vdots \\ B_l &:= \{A_{1l}, A_{2l}, \dots, A_{ll}\}. \end{aligned}$$

Clearly the sets $\Delta_{[M]}$ are disjoint and their union is $I^{(k,l)} \times I^{(k,l)}$. Note that the condition that $I_{AB} \in [M]$ is equivalent to the existence of $l \times l$ permutation matrices P and Q such that $I_{AB} = PMQ$. Thus to prove part 2, it remains to show that the pairs (A, B) and (C, D) lie in the same orbital if and only if there exist $l \times l$ permutation matrices P and Q such that $I_{CD} = PI_{AB}Q$. Write $A = A_1 | \dots | A_l$, $B = B_1 | \dots | B_l$, $C = C_1 | \dots | C_l$, and $D = D_1 | \dots | D_l$. Suppose (A, B) and (C, D) lie in the same orbital. Then there exists $g \in S_n$ such that $A^g = C$ and $B^g = D$. Let $C' = C'_1 | \dots | C'_l$ be the partition C but with the components C_i permuted in such a way that $A_i^g = C'_i$. Similarly, let D' be the partition $D = D'_1 | \dots | D'_l$ but with the components D_i permuted in such a way that $B_i^g = D'_i$. Then there exist permutation matrices P^{-1} and Q^{-1} such that $I_{C'D'} = P^{-1}I_{CD}Q^{-1}$. Now for any $i, j \in \{1, \dots, l\}$, we have that $|C'_i \cap D'_j| = |A_i \cap B_j|$, and hence $I_{CD} = PI_{C'D'}Q = PI_{AB}Q$. For the converse, suppose $I_{CD} = PI_{AB}Q$ for some $l \times l$ permutation matrices P and Q . Then after permuting the A_i 's and B_j 's suitably we may suppose $I_{AB} = I_{CD}$. Now since S_n is n -transitive, we can pick $g \in S_n$ such that $(A_i \cap B_j)^g = C_i \cap D_j$ for all $i, j \in \{1, \dots, l\}$ (note that $|\cup_{i,j \in \{1, \dots, l\}} (A_i \cap B_j)| = n$). Then $(A, B)^g = (C, D)$, and so (A, B) and (C, D) lie in the same orbital. This proves part 2. $\square$

Remark 3.2.4.

1. Again, the proof of Theorem 3.1.1 asserts that every maximal subgroup of S_{kl} which is transitive but not primitive is the stabiliser of a (k, l) -

partition of $\{1, \dots, kl\}$ and thus by Proposition 3.2.3(1), for fixed k and l , all such maximal subgroups are conjugate in S_{kl} .

2. For $\Delta_{[M]}$ as in Proposition 3.2.3, the paired orbital is $\Delta_{[M^T]}$, and hence $\Delta_{[M]}$ is self-paired if and only if $[M] = [M^T]$, which is not always the case. If it is the case, then the corresponding orbital graph will be denoted by $\Gamma_{[M]}$, and is the graph that has vertex set $I^{(k,l)}$ and edges $\{A, B\}$ where $I_{AB} \in [M]$.
3. The natural action of $H := A_{kl}$ on $I^{(k,l)}$ is also transitive and for $A \in I^{(k,l)}$, we have $H_A = G_A \cap H$ where $G := S_{kl}$. Since H_A is not maximal in H for $(k, l) = (2, 4)$ (see Theorem 3.1.1), when analysing this case, we will assume that $(k, l) \neq (2, 4)$. Note that A_{kl} is not necessarily transitive on all the orbitals $\Delta_{[M]}$ of $(S_{kl}, I^{(k,l)})$ (see Lemma 3.4.22(2) for an example).

We point out that in the case where $H <_{\max} S_n$ and H is primitive on I , we will assume that $H \neq A_n$, since $\text{diam}_O(G, (G : A_n)) = 1$, for any n . All groups appearing in Tables 3.2, 3.3, 3.9 and 3.10 have been denoted using standard notation; definitions of specific groups can be found in texts such as [24] or [9].

We now state the main results of the chapter.

Theorem 3.2.5. *Let (G, Ω) be a finite primitive permutation group where $G := S_n$ or $G := A_n$. Suppose there exists an integer $c \geq 1$ such that $\text{diam}_O(G, \Omega) \leq c$.*

1. *If $\Omega = I^{\{k\}}$, where $1 \leq k < n/2$, then $k \leq c$.*
2. *If $\Omega = I^{(k,l)}$, where $n = kl$ with $l > 1$ and $k > 1$, then $l \leq 2c$ and $k \leq 2c + 1$, and in particular, $n \leq 2c(2c + 1)$.*
3. *If $\Omega = (G : H)$, where $H \neq A_n$ is primitive on I , then $n < 2^{\epsilon(c+1)+3}$ with $\epsilon := 1.04$.*

For particular values of the bound c it is possible to be more specific about the precise actions that occur in Theorem 3.2.5. Here is such a result where $c = 5$.

Theorem 3.2.6. *Let (G, Ω) be a finite primitive permutation group where $G := S_n$ or $G := A_n$.*

1. *If $\Omega = I^{\{k\}}$, where $1 \leq k < n/2$, then $\text{diam}_O(G, \Omega) \leq 5$ if and only if $k \leq 5$.*
2. *If $\Omega = I^{(k,l)}$, where $n = kl$ with $l > 1$ and $k > 1$, then $\text{diam}_O(G, \Omega) \leq 5$ if and only if (k, l) are given in Table 3.1.*

l	2	3	4	5	6
k	≤ 11	≤ 5	≤ 3	2	2

Table 3.1: Pairs (k, l) with $\text{diam}_O(G, I^{(k,l)}) \leq 5$

3. *If $\Omega = (G : H)$, where $H \neq A_n$ is primitive on I , then $\text{diam}_O(G, \Omega) \leq 5$ if and only if the values of n and H are given in Tables 3.2 and 3.3; where the ‘if’ direction is only known to hold for values of $n \leq 12$ (see Remark 3.2.7(1)).*

n	H	Rank	Diameters of orbital graphs	Valencies of orbital graphs
5	$\text{AGL}_1(5)$	2	1	5
6	$\text{PGL}_2(5)$	2	1	5
7	$\text{AGL}_1(7)$	7	3, 3, 3, 2, 2, 2	7, 14, 14, 21, 21, 42
8	$\text{PGL}_2(7)$	5	3, 2, 2, 2	14, 21, 28, 56
9	$\text{AGL}_2(3)$	9	5, 3, 3, 3, 3, 2, 2, 2	8, 27, 36, 48, 144, 216, 216
10	$\text{PFL}_2(9)$	10	4, 4, 3, 3, 3, 2, 2, 2, 2	20, 45, 90, 144, 180, 240, 360, 720, 720
14	$\text{PGL}_2(13)$	19299	?	?
18	$\text{PGL}_2(17)$	?	?	?

Table 3.2: Pairs (n, H) with $\text{diam}_O(S_n, \Omega) \leq 5$, where $\Omega := (S_n : H)$ and H is primitive

n	H	Rank	Diameters of orbital graphs	Valencies of orbital graphs
5	D_{10}	2	1	5
6	$\text{PSL}_2(5)$	2	1	5
7	$\text{PSL}_3(2)$	2	1	14
8	$\text{ASL}_3(2)$	2	1	14
9	$\text{ASL}_2(3)$	12	5, 3, 3, 3, 3, 2, 3, 2, 2	8, 48, 27, 36, 72, 144, 72, 216, 216
9	$\text{PFL}_2(8)$	3	2, 2	56, 63
10	M_{10}	12	4, 4, 3, 3, 3, 3, 2, 2, 2, 2	20, 45, 90, 90, 90, 144, 240, 360, 720, 720
11	M_{11}	5	2, 2, 2, 2	110, 330, 495, 1584
12	M_{12}	4	2, 2, 2	440, 495, 1584
14	$\text{PSL}_2(13)$	?	?	?
17	$\text{PFL}_2(16)$	?	?	?
23	M_{23}	?	?	?
24	M_{24}	?	?	?

Table 3.3: Pairs (n, H) with $\text{diam}_O(A_n, \Omega) \leq 5$, where $\Omega := (A_n : H)$ and H is primitive

Remark 3.2.7.

1. Tables 3.2 and 3.3 contain six cases with $n = 14, 17, 18, 23$ or 24 , marked with question marks, where we have been unable to compute the diameters of any orbital graphs.
2. The groups appearing in the rows corresponding to $n = 5, 6, 9$ (first row), 10 and 14 in Table 3.3 are just the intersections of the corresponding groups appearing in Table 3.2 with A_n , in other words, these groups *extend* to maximal subgroups of S_n . The groups appearing in the remaining rows of Table 3.3 do not extend to maximal subgroups of S_n .

We also analyse orbital graphs of diameter 2 of the primitive permutations groups (S_n, Ω) and (A_n, Ω) . For the case where $\Omega \neq I^{(k,l)}$, we find all orbital graphs of diameter 2. For $\Omega = I^{(k,l)}$, we find an example of an infinite family of orbital graphs of diameter 2; there could be more infinite families of orbital graphs of diameter 2, but classifying all of them could take significantly more effort.

Theorem 3.2.8. *Let (G, Ω) be a finite primitive permutation group where $G := S_n$ or $G := A_n$.*

1. *If $\Omega = I^{\{k\}}$, where $1 < k < n/2$, then $\text{diam}(\Gamma_{n,k,i}) = 2$ if and only if one of the following holds:*
 - $i = 0$ and $n \geq 3k - 1$;
 - $i \in \{1, \dots, \lfloor k/2 \rfloor\}$ and $n \geq 3k - 2i$.
2. *If $\Omega = I^{(k,k)}$ with $n = k^2 \geq 9$ and $G = S_n$, let $\Gamma_{[M]}$ be the orbital graph where M is the $k \times k$ matrix with all entries equal to 1. Then $\text{diam}(\Gamma_{[M]}) = 2$. If $G = A_{k^2}$ and either k is odd, or k is even and $k/2$ is odd, then $\Gamma_{[M]}$ is also an orbital graph of $(G, I^{(k,k)})$.*

3. If $\Omega = (G : H)$, where H is primitive on I , then Tables 3.4 and 3.5 specify the values of n and H for which (G, Ω) has an orbital graph of diameter 2 (the case $n = 24$ is still just a possibility; see Remark 3.2.9(1)).

n	H	Rank	$ \mathcal{D}_2 $	Valencies of orbital graphs of diameter 2
7	$\text{AGL}_1(7)$	7	3	21, 21, 42
8	$\text{PGL}_2(7)$	5	3	21, 28, 56
9	$\text{AGL}_2(3)$	9	3	144, 216, 216
10	$\text{PFL}_2(9)$	10	4	240, 360, 720, 720

Table 3.4: Pairs (n, H) such that (S_n, Ω) has an orbital graph of diameter 2, where $\Omega := (S_n : H)$ and H is primitive

n	H	Rank	$ \mathcal{D}_2 $	Valencies of orbital graphs of diameter 2
9	$\text{ASL}_2(3)$	12	3	144, 216, 216
9	$\text{PFL}_2(8)$	3	2	56, 63
10	M_{10}	12	4	240, 360, 720, 720
11	M_{11}	5	4	110, 330, 495, 1584
12	M_{12}	4	3	440, 495, 1584
13	$\text{PSL}_3(3)$	126	28	$5616^{[3]}, 11232^{[25]}$
15	$\text{PSL}_4(2)$	1687	≥ 8	$40320^{[8]}, \dots$
16	$2^4.\text{PSL}_4(2)$	151	79	$40320^{[1]}, 80640^{[2]}, 53760^{[1]}, 64512^{[1]}, 161280^{[7]}, 107520^{[3]}, 322560^{[39]}, 645120^{[25]}$
24	M_{24}	?	?	?

Table 3.5: Pairs (n, H) such that (A_n, Ω) has an orbital graph of diameter 2, where $\Omega := (A_n : H)$ and H is primitive

Remark 3.2.9.

1. In Table 3.5, $\mathcal{D}_2$ denotes the set of orbital graphs of diameter 2. In the ‘valencies’ column of the table, the notation $x^{[y]}$ has been used to

denote that the valency x appears y times. This table contains the case $n = 24$ which is marked with a question mark since we have been unable to determine or disprove the existence of an orbital graph of diameter 2 for this case.

2. The groups appearing in the rows corresponding to $n = 9$ (first row) and $n = 10$ in Table 3.5 are just the intersections of the corresponding groups appearing in Table 3.4 with A_n . The groups appearing in the remaining rows of Table 3.5 do not extend to maximal subgroups of S_n .

3.3 Action of S_n on $I^{\{k\}}$

In this section we prove Theorems 3.2.5(1), 3.2.6(1) and 3.2.8(1). Recall that the orbital graph $\Gamma_{n,k,i}$ has vertices which are the k -subsets of $\{1, \dots, n\}$ and edges $\{A, B\}$ where $|A \cap B| = i$. The methods used to prove Theorem 3.2.8(1) can be extended to find the diameters of all of the graphs $\Gamma_{n,k,i}$, and so we also prove a result on this (see Theorem 3.3.1). Some work has already been done in [7] on finding the diameters of the graphs $\Gamma_{n,k,i}$. However, we believe that the main result in [7] has an error, and state the correct result below.

Theorem 3.3.1. *Let $k \geq 1$ and $n \geq 2k + 1$ be integers.*

1. $\text{diam}(\Gamma_{n,k,0}) = \lceil \frac{n-k-1}{n-2k} \rceil$.
2. For $i \in \{1, \dots, \lfloor k/2 \rfloor\}$,
 - (a) $\text{diam}(\Gamma_{n,k,i}) = 2 \Leftrightarrow n \geq 3k - 2i$.
 - (b) $\text{diam}(\Gamma_{n,k,i}) = 3 \Leftrightarrow \frac{5(k-i)-1}{2} \leq n < 3k - 2i$.
 - (c) $\text{diam}(\Gamma_{n,k,i}) = \lceil \frac{n-k+i-1}{n-2k+2i} \rceil > 3 \Leftrightarrow n < \frac{5(k-i)-1}{2}$.
3. For $i > \lfloor k/2 \rfloor$, $\text{diam}(\Gamma_{n,k,i}) = \lceil \frac{k}{k-i} \rceil$.

The error occurs in line 2 on p. 6648 of [7]. According to [7], the orbital graph $\Gamma_{n,k,i}$ has diameter 3 for any $i > \lfloor k/2 \rfloor$, and Theorem 7 specifies a construction of a path of length 3 between any two vertices A and B with $m := |A \cap B| < 2i - k$. This involves constructing a set $Z = Z(n, k, i, m)$ which is however impossible to construct for many values of n, k, i and m ; for example, let $(n, k, i, m) := (2k + 1, k, k - 1, 0)$, where $k \geq 4$, then $|Z| = 2k - 3i + m = 3 - k \leq -1$. In fact it can be observed that in the particular case where $i = k - 1$, we have $\text{diam}(\Gamma_{n,k,k-1}) = k$.

We now state and prove a result from which Theorems 3.2.5(1) and 3.2.6(1) will follow.

Proposition 3.3.2. *Let (G, Ω) be a finite primitive permutation group where $G := S_n$ or A_n , and let $\Omega = I^{\{k\}}$ with $1 \leq k < n/2$. Then $\text{diam}_O(G, \Omega) \leq c$ if and only if $k \leq c$.*

Proof. Suppose $\text{diam}_O(G, \Omega) \leq c$. Recall that in the orbital graph $\Gamma_{n,k,k-1}$, two k -subsets are joined by an edge if they intersect in $k - 1$ points. Observe that this graph has diameter k , and so $k \leq \text{diam}_O(G, \Omega) \leq c$. Conversely, suppose $k \leq c$ and let Γ be an orbital graph of (G, Ω) . For a k -subset A and an integer $j \geq 1$ define

$$\Delta_j(A) := \{B : d(A, B) = j\}.$$

If $B \in \Delta_j(A)$ and $g \in G_A$, then $B^g \in \Delta_j(A)$, hence $B^{G_A} \subseteq \Delta_j(A)$. Therefore $\Delta_j(A)$ is a union of non-trivial orbits of G_A on Ω . The number of non-trivial orbits of G_A on Ω is the number of non-diagonal orbitals, which is k by Proposition 3.2.1(2), and therefore $\text{diam}(\Gamma) \leq k \leq c$. This implies $\text{diam}_O(G, \Omega) \leq c$. $\square$

Proof of Theorems 3.2.5(1) and 3.2.6(1). Theorem 3.2.5(1) is the ‘only if’ implication of Proposition 3.3.2, and Theorem 3.2.6(1) is the $c = 5$ case of Proposition 3.3.2. $\square$

We now work towards proving Theorem 3.2.8(1). Henceforth, for a graph Γ , we will use $V(\Gamma)$ to denote the vertex-set of Γ . The following lemma follows from Lemmas 1 and 2 from [8] and the fact that $\Gamma_{n,k,i}$ is a subgraph of the graph $K(n, k, i)$ from [8].

Lemma 3.3.3. *Let $n \geq 2k$, $i \in \{0, \dots, k-1\}$ and $A, B \in V(\Gamma_{n,k,i})$. Let $r \geq 1$.*

1. *If A and B are connected by a path of length $2r$, then*

$$|A \cap B| \geq (2r+1)k - rn - 2ri,$$

2. *If A and B are connected by a path of length $2r+1$, then*

$$|A \cap B| \leq rn - 2rk + (2r+1)i.$$

Lemma 3.3.4. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$, and $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$. Then*

$$d(A, B) = 2 \Leftrightarrow m \geq 3k - n - 2i.$$

In particular, if $n \geq 3k - 2i$, then $d(A, B) = 2$.

Proof. If $d(A, B) = 2$, then by Lemma 3.3.3(1) we have $m \geq 3k - n - 2i$. Conversely, suppose $m \geq 3k - n - 2i$. Recall that $I = \{1, \dots, n\}$. If $i \leq k - m$, then choose a k -subset C consisting of i elements from $A \setminus B$, i elements from $B \setminus A$, and $k - 2i$ elements from $I \setminus (A \cup B)$ (note that $|I \setminus (A \cup B)| \geq k - 2i$, since $n \geq 3k - m - 2i$). If $i > k - m$, then choose a k -subset C consisting of $i - k + m$ elements from $A \cap B$, $k - m$ elements from $A \setminus B$, $k - m$ elements from $B \setminus A$, and $m - i$ elements from $I \setminus (A \cup B)$ (note that $|I \setminus (A \cup B)| \geq m - i$ since $n \geq 2k - i$). Then $A - C - B$ is a path of length 2, and hence $d(A, B) = 2$. Now suppose $n \geq 3k - 2i$. Then $m \geq 0 \geq 3k - n - 2i$. Hence $d(A, B) = 2$ by the first part. $\square$

Corollary 3.3.5. *Let $n \geq 2k$ and $i \in \{0, \dots, \lfloor k/2 \rfloor\}$. Suppose we have that $\text{diam}(\Gamma_{n,k,i}) \geq 3$. Then $n < 3k - 2i$ and for $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$,*

$$d(A, B) > 2 \Leftrightarrow m < 3k - n - 2i.$$

Proof of Theorem 3.2.8(1) and Theorem 3.3.1(2a). Note that $\text{diam}(\Gamma_{n,k,i}) = 2$ if and only if for all $A \neq B \in V(\Gamma_{n,k,i})$ such that $|A \cap B| \neq i$, it holds that $d(A, B) = 2$. Hence by Lemma 3.3.4, $\text{diam}(\Gamma_{n,k,0}) = 2$ if and only if either $n \geq 3k$ or $3k - n = 1$, and if $i \in \{1, \dots, \lfloor k/2 \rfloor\}$, then $\text{diam}(\Gamma_{n,k,i}) = 2$ if and only if $n \geq 3k - 2i$. Now suppose $i > \lfloor k/2 \rfloor$ and let $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| = 0$. If C is a common neighbour of A and B , then $|C| \geq 2i > k$ which contradicts the fact that $|C| = k$. Hence $d(A, B) > 2$ and $\text{diam}(\Gamma_{n,k,i}) \geq 3$. $\square$

We now continue proving the rest of Theorem 3.3.1. To do so, we will need the following result.

Lemma 3.3.6. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$ and $d := \text{diam}(\Gamma_{n,k,i})$. Suppose $d \geq 3$. Let $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$. Then for $v \in \{3, \dots, d\}$,*

$$P(v) : \quad d(A, B) = v \Leftrightarrow f(n, k, i, v) \leq m \leq g(n, k, i, v),$$

where f and g are as in Tables 3.6 and 3.7, for v even and v odd respectively.

n		
	$< \frac{(2v-1)(k-i)}{v-1}$	$\geq \frac{(2v-1)(k-i)}{v-1}$
f	$(2r+1)k - rn - 2ri$	$(r-1)n - (2r-2)k + (2r-1)i + 1$
g	$(2r-1)k - (r-1)n - (2r-2)i - 1$	

Table 3.6: Criterion for distance $v = 2r$ in the graph $\Gamma_{n,k,i}$, where $r \geq 2$

	n	
	$< \frac{(2v-1)(k-i)}{v-1}$	$\geq \frac{(2v-1)(k-i)}{v-1}$
f	$0, r = 1$ $(r-1)n - (2r-2)k + (2r-1)i + 1, r \geq 2$	
g	$rn - 2rk + (2r+1)i$	$(2r+1)k - rn - 2ri - 1$

Table 3.7: Criterion for distance $v = 2r + 1$ in the graph $\Gamma_{n,k,i}$, where $r \geq 1$

In order to prove Lemma 3.3.6, we now prove the following sequence of results.

Lemma 3.3.7. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$ and $t \geq 3$. Suppose the following conditions hold:*

1. $\text{diam}(\Gamma_{n,k,i}) \geq t + 1$,
2. $n < \frac{(2t-1)(k-i)}{t-1}$,
3. $P(v)$ holds for all $v \in \{3, \dots, t\}$.

Let $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$. Then for t even ($t = 2r$),

$$d(A, B) > 2r \Leftrightarrow (r-1)n - (2r-2)k + (2r-1)i < m < (2r+1)k - rn - 2ri,$$

and for t odd ($t = 2r + 1$),

$$d(A, B) > 2r + 1 \Leftrightarrow rn - 2rk + (2r+1)i < m < (2r+1)k - rn - 2ri.$$

Remark 3.3.8. By Lemma 3.3.9 (see below), if (1) and (3) of Lemma 3.3.7 hold then so does (2), hence after Lemma 3.3.9 has been proved we may omit (2) from the statement of Lemma 3.3.7. Similarly, after Lemma 3.3.6 has been proved, we may also omit (3).

Proof of Lemma 3.3.7. We proceed by induction on t . For the base case suppose the conditions of the lemma hold for $t = 3$. Then by Corollary 3.3.5

and $P(3)$,

$$d(A, B) = 3 \Leftrightarrow 0 \leq m \leq n - 2k + 3i,$$

$$d(A, B) = 2 \Leftrightarrow m \geq 3k - n - 2i,$$

from which the result for $t = 3$ follows. Now let $t = 2r > 3$ and suppose the lemma holds for $t - 1$. Suppose also that the conditions of the lemma hold for t . Then the conditions of the lemma also hold for $t - 1$, and so by the inductive assumption,

$$\begin{aligned} d(A, B) > 2r - 1 &\Leftrightarrow (r - 1)n - (2r - 2)k + (2r - 1)i < m \\ &< (2r - 1)k - (r - 1)n - (2r - 2)i. \end{aligned} \quad (3.1)$$

Now by $P(2r)$, we have that

$$\begin{aligned} d(A, B) = 2r &\Leftrightarrow (2r + 1)k - rn - 2ri \leq m \\ &\leq (2r - 1)k - (r - 1)n - (2r - 2)i - 1. \end{aligned} \quad (3.2)$$

We obtain the result for $t = 2r$ by combining (3.1) and (3.2). To complete the induction, it remains to show the result for $t + 1 = 2r + 1$ which can be done using similar arguments to the above and is left to the reader. $\square$

Lemma 3.3.9. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$ and $t \geq 3$. Suppose $P(v)$ holds for all $v \in \{3, \dots, t\}$ and $\text{diam}(\Gamma_{n,k,i}) \geq t + 1$. Then*

$$n < \frac{(2t - 1)(k - i)}{t - 1}.$$

Proof. We proceed by induction on t . For the base case, assume $P(3)$ holds and $\text{diam}(\Gamma_{n,k,i}) \geq 4$. Suppose $n \geq \frac{5(k-i)}{2}$. Then using Corollary 3.3.5 and $P(3)$ we see that $d(A, B) \leq 3$ for all $A, B \in V(\Gamma_{n,k,i})$, which contradicts the fact that $\text{diam}(\Gamma_{n,k,i}) \geq 4$. Hence $n < \frac{5(k-i)}{2}$. This completes the base case. Now let $t = 2r \geq 4$ and assume the lemma holds for $t - 1$. Suppose $P(v)$ holds for all $v \in \{3, \dots, t\}$ and $\text{diam}(\Gamma_{n,k,i}) \geq t + 1$. Then $P(v)$ holds for all $v \in \{3, \dots, t - 1\}$ and $\text{diam}(\Gamma_{n,k,i}) \geq t$, hence by the inductive assumption we have $n < \frac{(2t-3)(k-i)}{t-2}$. Thus (3.1) holds by Lemma 3.3.7. Suppose $n \geq \frac{(2t-1)(k-i)}{t-1}$. Then using (3.1) and $P(2r)$ we see that $d(A, B) \leq 2r$, for all $A, B \in V(\Gamma_{n,k,i})$, which contradicts the fact that $\text{diam}(\Gamma_{n,k,i}) \geq 2r + 1$. Hence $n < \frac{(2t-1)(k-i)}{t-1}$. To complete the induction, it remains to show the result for $t + 1 = 2r + 1$ which can be done using similar arguments to the above and is left to the reader. $\square$

Lemma 3.3.10. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$ and suppose that we have $\text{diam}(\Gamma_{n,k,i}) \geq 3$. Let $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$. If $n < \frac{5(k-i)}{2}$, then*

$$d(A, B) = 3 \Leftrightarrow 0 \leq m \leq n - 2k + 3i,$$

and if $n \geq \frac{5(k-i)}{2}$, then

$$d(A, B) = 3 \Leftrightarrow 0 \leq m \leq 3k - n - 2i - 1.$$

Proof. Suppose $n < \frac{5(k-i)}{2}$. If $d(A, B) = 3$, then by Lemma 3.3.3(2) we have $m \leq n - 2k + 3i$. For the converse, assume $m \leq n - 2k + 3i$. Since $n < \frac{5(k-i)}{2}$, we have that $m < 3k - n - 2i$, and so by Corollary 3.3.5 we have $d(A, B) > 2$. Choose a neighbour A_1 of A such that $|A_1 \cap B|$ is maximal. If $i < m$, then $|A_1 \cap B| = i + k - m$, and if $i > m$, then $|A_1 \cap B| = m + k - i$. In both cases (for $i < m$ use $m \leq n - 2k + 3i$, and for $i > m$ use $m \geq 0$) we have $|A_1 \cap B| \geq 3k - 2i - n$. Hence by Lemma 3.3.4 we have $d(A_1, B) = 2$, and so $d(A, B) = 3$. Now suppose $n \geq \frac{5(k-i)}{2}$. If $d(A, B) = 3$, then by Corollary 3.3.5 we have $m < 3k - n - 2i$. For the converse, assume $m < 3k - n - 2i$. Then

by Corollary 3.3.5 we have $d(A, B) > 2$, and using the fact that $n \geq \frac{5(k-i)}{2}$, we see that $m \leq n - 2k + 3i$. Now, we show that $d(A, B) = 3$ by constructing a path of length 3 between A and B , as above. $\square$

Corollary 3.3.11. *Let $n > 2k$. We have*

$$\text{diam}(\Gamma_{n,k,0}) = 3 \Leftrightarrow \frac{5k-1}{2} \leq n < 3k-1,$$

and for $i \in \{1, \dots, \lfloor k/2 \rfloor\}$, we have

$$\text{diam}(\Gamma_{n,k,i}) = 3 \Leftrightarrow \frac{5(k-i)-1}{2} \leq n < 3k-2i.$$

Proof. Suppose $\text{diam}(\Gamma_{n,k,0}) = 3$. By Theorem 3.2.8(1) we have $n < 3k-1$. By Corollary 3.3.5, for $A, B \in V(\Gamma_{n,k,0})$ with $m := |A \cap B| \neq 0$, we have

$$d(A, B) > 2 \Leftrightarrow m < 3k - n. \quad (3.3)$$

Now $\text{diam}(\Gamma_{n,k,0}) = 3$ implies that for all $A, B \in V(\Gamma_{n,k,0})$ with $d(A, B) > 2$, we must have $d(A, B) = 3$. Thus using Lemma 3.3.10, we deduce that either $n \geq \frac{5k}{2}$ or $3k - n - 1 = n - 2k$, i.e. $n \geq \frac{5k-1}{2}$. Conversely, suppose $\frac{5k-1}{2} \leq n < 3k-1$. Then by Theorem 3.2.8(1) we have $\text{diam}(\Gamma_{n,k,0}) \geq 3$. Hence by Corollary 3.3.5, for $A, B \in V(\Gamma_{n,k,0})$ with $m := |A \cap B| \neq 0$, we have (3.3). Now Lemma 3.3.10 and the fact that $n \geq \frac{5k-1}{2}$, imply $d(A, B) \leq 3$ for all $A, B \in V(\Gamma_{n,k,0})$. Hence $\text{diam}(\Gamma_{n,k,0}) = 3$. This proves the first statement. The second statement can be proved similarly and is left to the reader. $\square$

Proof of Theorem 3.3.1(2b). See Corollary 3.3.11. $\square$

We need one final result before we can prove Lemma 3.3.6.

Lemma 3.3.12. *Let $n \geq 2k$, $i \in \{0, \dots, \lfloor k/2 \rfloor\}$ and $r \geq 2$. Let $A, B \in V(\Gamma_{n,k,i})$ where $m := |A \cap B| \neq i$.*

1. *Suppose $d(A, B) \geq 2r$, $P(v)$ holds for $v \in \{3, \dots, 2r-1\}$, and*

$$(2r+1)k - rn - 2ri \leq m < (2r-1)k - (r-1)n - (2r-2)i. \quad (3.4)$$

Then $d(A, B) = 2r$.

2. Suppose $d(A, B) \geq 2r + 1$, $P(v)$ holds for $v \in \{3, \dots, 2r\}$, and

$$(r - 1)n - (2r - 2)k + (2r - 1)i < m \leq rn - 2rk + (2r + 1)i. \quad (3.5)$$

Then $d(A, B) = 2r + 1$.

Proof. Suppose the conditions in part 1 of the lemma hold. If $k - m < i$, then $m \geq 3k - n - 2i$ and so by Lemma 3.3.4 we have $d(A, B) = 2$ which is not possible since $d(A, B) \geq 2r \geq 4$. Therefore $k - m \geq i$. Choose a neighbour A_1 of A such that $|A_1 \cap B|$ is minimal. Since $k - m \geq i$, we have $|A_1 \cap B| = 3k - i - n - m$. Now rearranging (3.4) gives

$$(2r - 3)i + (r - 2)n - (2r - 4)k < |A_1 \cap B| \leq (2r - 1)i + (r - 1)n - (2r - 2)k.$$

Therefore using Lemma 3.3.9 (with $t = 2r - 1$) and $P(2r - 1)$ we have $d(A_1, B) = 2r - 1$, and hence $d(A, B) = 2r$. This proves the first part of the lemma. Now suppose the conditions in part 2 of the lemma hold. Choose a neighbour A_1 of A such that $|A_1 \cap B|$ is maximal. Then (3.5) implies $m > i$, and so $|A_1 \cap B| = i + k - m$. Now rearranging (3.5) implies

$$(2r + 1)k - rn - 2ri \leq |A_1 \cap B| < (2r - 1)k - (2r - 2)i - (r - 1)n.$$

Therefore using Lemma 3.3.9 (with $t = 2r$) and $P(2r)$ we have $d(A_1, B) = 2r$, and hence $d(A, B) = 2r + 1$. $\square$

Proof of Lemma 3.3.6. For $v = 3$, the result is proved in Lemma 3.3.10. For $v \geq 4$, we proceed by induction on v . Here $d = \text{diam}(\Gamma_{n,k,i}) \geq v$. Firstly, we prove the base case $v = 4$. Suppose $n < \frac{7(k-i)}{3}$. If $d(A, B) = 4$, then by Lemma 3.3.3(1) we have $m \geq 5k - 2n - 4i$. Since $d(A, B) > 2$, by Corollary 3.3.5 we also have $m < 3k - n - 2i$. For the converse, assume $5k - 2n - 4i \leq m < 3k - n - 2i$. Note that since $P(3)$ already holds, by Remark 3.3.8, in order to use Lemma 3.3.7 (with $t = 3$), we only need to ensure that $\text{diam}(\Gamma_{n,k,i}) \geq 4$, which is true by assumption. Now using

Lemma 3.3.7 and the fact that $n < \frac{7(k-i)}{3}$, we see that $d(A, B) > 3$, and so by Lemma 3.3.12 we have $d(A, B) = 4$. Now suppose $n \geq \frac{7(k-i)}{3}$. If $d(A, B) = 4$, then using Lemma 3.3.7 (with $t = 3$) we have $m > n - 2k + 3i$. Also $d(A, B) > 2$, so by Corollary 3.3.5 we have $m < 3k - n - 2i$. For the converse, assume $n - 2k + 3i < m < 3k - n - 2i$. Then using Lemma 3.3.7 we see that $d(A, B) > 3$. Now using the fact that $n \geq \frac{7(k-i)}{3}$ we have $5k - 2n - 4i \leq m < 3k - n - 2i$, and so by Lemma 3.3.12 we have $d(A, B) = 4$. This completes the base case.

Now let $r \geq 2$ and assume that $P(v)$ holds for all $v \in \{3, \dots, 2r\}$. We will show that $P(2r+1)$ holds. Suppose $n < \frac{(4r+1)(k-i)}{2r}$. If $d(A, B) = 2r+1$, then by Lemma 3.3.3(2) we have $m \leq rn - 2rk + (2r+1)i$. Since $d(A, B) > 2r-1$, by Lemma 3.3.7 we also have $m > (r-1)n - (2r-2)k + (2r-1)i$. For the converse, assume that

$$(r-1)n - (2r-2)k + (2r-1)i < m \leq rn - 2rk + (2r+1)i. \quad (3.6)$$

Then using Lemma 3.3.7 and the fact that $n < \frac{(4r+1)(k-i)}{2r}$ we have that $d(A, B) > 2r$, and so by Lemma 3.3.12 we have $d(A, B) = 2r+1$. Now suppose that $n \geq \frac{(4r+1)(k-i)}{2r-1}$. If $d(A, B) = 2r+1$, then using Lemma 3.3.7 (with $t = 2r$) we have $m < (2r+1)k - rn - 2ri$. Since $d(A, B) > 2r-1$, by Lemma 3.3.7 we also have $m > (r-1)n - (2r-2)k + (2r-1)i$. For the converse, assume that

$$(r-1)n - (2r-2)k + (2r-1)i < m < (2r+1)k - rn - 2ri.$$

Then using Lemma 3.3.7 we have $d(A, B) > 2r$. Now using the fact that $n \geq \frac{(4r+1)(k-i)}{2r-1}$ we see that (3.6) holds, and so by Lemma 3.3.12 we have $d(A, B) = 2r+1$. This shows $P(2r+1)$. To complete the induction, it remains to show $P(2r+2)$ which can be done using similar arguments to the above and is left to the reader. $\square$

Proof of Theorem 3.3.1(1) and (2c). It follows from Theorem 3.2.8(1) and Corollary 3.3.11, that Theorem 3.3.1(1) holds when $\text{diam}(\Gamma_{n,k,0})$ is 2 or 3. For $t \geq 4$, an equivalent restatement of Theorem 3.3.1(1) and (2c) is that for $i \in \{0, \dots, \lfloor k/2 \rfloor\}$,

$$R(t) : \quad \text{diam}(\Gamma_{n,k,i}) = t \Leftrightarrow \frac{(2t-1)(k-i)-1}{t-1} \leq n < \frac{(2t-3)(k-i)-1}{t-2}. \quad (3.7)$$

We prove (3.7) by induction on t . The base case will be to show that

$$\text{diam}(\Gamma_{n,k,i}) = 4 \Leftrightarrow \frac{7(k-i)-1}{3} \leq n < \frac{5(k-i)-1}{2}. \quad (3.8)$$

Suppose $\text{diam}(\Gamma_{n,k,i}) = 4$. Then by Theorem 3.2.8(1) and Corollary 3.3.11, $n < \frac{5(k-i)-1}{2}$. By Lemma 3.3.7, for $A, B \in V(\Gamma_{n,k,i})$ with $m := |A \cap B| \neq i$, we have

$$d(A, B) > 3 \Leftrightarrow n - 2k + 3i < m < 3k - n - 2i. \quad (3.9)$$

Now $\text{diam}(\Gamma_{n,k,i}) = 4$ implies that for all $A, B \in V(\Gamma_{n,k,i})$ with $d(A, B) > 3$, we must have $d(A, B) = 4$. Thus since $P(4)$ holds by Lemma 3.3.6, using $P(4)$ we obtain that either $n \geq \frac{7(k-i)-1}{3}$ or $n - 2k + 3i + 1 = 5k - 2n - 4i$, i.e. $n \geq \frac{7(k-i)-1}{3}$. Conversely, suppose that the right hand side of (3.8) holds. Since $n < \frac{5(k-i)-1}{2}$, by Theorem 3.2.8(1) and Corollary 3.3.11 we have $\text{diam}(\Gamma_{n,k,i}) \geq 4$, and by Lemma 3.3.7 we see that (3.9) holds. Now using (3.9), $P(4)$ and the fact that $n \geq \frac{7(k-i)-1}{3}$, we obtain that for all $A, B \in V(\Gamma_{n,k,i})$ with $d(A, B) > 3$, we have $d(A, B) = 4$, and thus $\text{diam}(\Gamma_{n,k,i}) = 4$. This completes the base case.

Now let $r \geq 3$ and suppose $R(t)$ holds for all $t \in \{4, \dots, 2r-2\}$. We will show that $R(2r-1)$ holds. Suppose $\text{diam}(\Gamma_{n,k,i}) = 2r-1$. Then by Theorem 3.2.8(1), Corollary 3.3.11 and the inductive assumption, we have $n < \frac{(4r-5)(k-i)-1}{2r-3}$. Now by Lemma 3.3.7, for $A, B \in V(\Gamma_{n,k,i})$ with $m :=$

$|A \cap B| \neq i$, we have

$$\begin{aligned} d(A, B) > 2r - 2 &\Leftrightarrow (r - 2)n - (2r - 4)k + (2r - 3)i < m \\ &< (2r - 1)k - (r - 1)n - (2r - 2)i. \end{aligned} \quad (3.10)$$

Now $\text{diam}(\Gamma_{n,k,i}) = 2r - 1$ implies that for all $A, B \in V(\Gamma_{n,k,i})$ with $d(A, B) > 2r - 2$, we must have $d(A, B) = 2r - 1$. Hence using $P(2r - 1)$, we obtain that either $(2r - 2)n \geq (4r - 3)(k - i)$, or

$$(2r - 1)k - (r - 1)n - (2r - 2)i - 1 = (r - 1)n - (2r - 2)k + (2r - 1)i.$$

Conversely, suppose that the right hand side of (3.7) holds with $t = 2r - 1$. Since $n < \frac{(4r-5)(k-i)-1}{2r-3}$, using Theorem 3.2.8(1), Corollary 3.3.11 and the inductive assumption we have $\text{diam}(\Gamma_{n,k,i}) \geq 2r - 1$, and by Lemma 3.3.7 we see that (3.10) holds. Now using (3.10), $P(2r - 1)$ and the fact that $n \geq \frac{(4r-3)(k-i)-1}{2r-2}$, we obtain that for all $A, B \in V(\Gamma_{n,k,i})$ with $d(A, B) > 2r - 2$, we have $d(A, B) = 2r - 1$, and thus $\text{diam}(\Gamma_{n,k,i}) = 2r - 1$. This shows $R(2r - 1)$. To complete the induction, it remains to show $R(2r)$ which can be shown using similar arguments to the above and is left to the reader. $\square$

We now prove some results required to prove Theorem 3.3.1(3).

Lemma 3.3.13. *Let $n \geq 2k$ and $i \in \{\lfloor k/2 \rfloor + 1, \dots, k - 1\}$, and suppose $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| =: m > i$. Then $d(A, B) = 2$.*

Proof. Since $m > i$, we can choose a k -subset C containing i elements from $A \cap B$, and since $i > k/2$ implies $|I \setminus (A \cup B)| = n - 2k + m \geq m > i > k - i$, we can also choose C to contain $k - i$ elements from $I \setminus (A \cup B)$. Then $|C| = k$ and $A - C - B$ is a path of length 2, and hence $d(A, B) = 2$. $\square$

Now let $n \geq 2k$ and $i \in \{\lfloor k/2 \rfloor + 1, \dots, k - 1\}$, and suppose that $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| = m < i$. Let j_m be the least positive

integer such that $j_m(k-i) + m \geq i$, i.e. $j_m = \lceil \frac{i-m}{k-i} \rceil$. Construct a path

$$A - A_1 - \cdots - A_{j_m}, \quad (3.11)$$

where we define $A_0 := A$, and for $l \in \{1, \dots, j_m\}$, A_l is chosen so that $|A_{l-1} \cap A_l| = i$ and $|A_l \cap B|$ is maximal.

Lemma 3.3.14. *Let $n \geq 2k$ and $i \in \{\lfloor k/2 \rfloor + 1, \dots, k-1\}$, and suppose $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| =: m < i$. Then $d(A, B) \leq j_m + 1 = \lceil \frac{k-m}{k-i} \rceil$.*

Proof. Consider the path in (3.11) and observe that $|A_l \cap B| = |A_{l-1} \cap B| + (k-i) = m + l(k-i)$, for any $l \in \{1, \dots, j_m\}$. If $j_m(k-i) + m = i$, then $|A_{j_m} \cap B| = i$. Hence $A - A_1 - \cdots - A_{j_m} - B$ is a path of length $j_m + 1$. Now, if $|A_{j_m} \cap B| = j_m(k-i) + m > i$, then let $\alpha := j_m(k-i) + m - i > 0$. Since $i > k/2$, this implies $|A_{j_m-1} \cup B| + \alpha = 3k - 2i < 2k \leq n$, and hence we can choose a vertex A'_{j_m} which is the vertex A_{j_m} but with α elements from $(A_{j_m} \cap B) \setminus (A_{j_m} \cap A_{j_m-1})$ replaced with α elements which are not in $A_{j_m-1} \cup B$. Then $A - A_1 - \cdots - A_{j_m-1} - A'_{j_m} - B$ is a path of length $j_m + 1$. Thus $d(A, B) \leq j_m + 1$. $\square$

We will now show that the inequality in Lemma 3.3.14 is in fact an equality.

Lemma 3.3.15. *Let $n \geq 2k$, $i \in \{\lfloor k/2 \rfloor + 1, \dots, k-1\}$ and $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| =: m$. Then $d(A, B) \geq \lceil \frac{k-m}{k-i} \rceil$.*

Proof. Suppose $d(A, B) = l+1$ and $A - C_1 - \cdots - C_l - B$ is a shortest path. It can be seen using a short inductive argument that C_l can differ from A by at most $l(k-i)$ points. This and the fact that $|C_l \cap B| \leq |A \cap B| + |C_l \setminus A|$ imply $|C_l \cap B| \leq m + l(k-i)$. On the other hand $|C_l \cap B| = i$ so $i \leq m + l(k-i)$. This implies

$$l + 1 \geq \frac{k-m}{k-i},$$

from which the claim follows. $\square$

Remark 3.3.16.

1. If $m > i$, then $0 < \frac{k-m}{k-i} < 1$, so Lemma 3.3.15 just states that $d(A, B) \geq 1$. However if $m < i$, then $\frac{k-m}{k-i} > 1$ and so Lemma 3.3.15 provides useful information about $d(A, B)$.
2. Lemma 3.3.15 also holds for $i \leq \lfloor k/2 \rfloor$. For $m > i$ this is obvious by part 1 of the remark. For $m < i$, this can be seen as follows. Since $m < i$, we have $d(A, B) \geq 2$. Also, $k - i \geq k/2$ which implies that

$$\frac{k-m}{k-i} \leq \frac{2(k-m)}{k} = 2 \left(1 - \frac{m}{k}\right) \leq 2.$$

Hence $d(A, B) \geq 2 \geq \frac{k-m}{k-i}$, from which the claim follows.

The following corollary is a consequence of Lemmas 3.3.14 and 3.3.15.

Corollary 3.3.17. *Let $n \geq 2k$ and $i \in \{\lfloor k/2 \rfloor + 1, \dots, k-1\}$, and suppose $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| := m < i$. Then $d(A, B) = \lceil \frac{k-m}{k-i} \rceil$.*

We now prove the last result of this section, namely Theorem 3.3.1(3).

Proof of Theorem 3.3.1(3). Suppose $A, B \in V(\Gamma_{n,k,i})$ with $|A \cap B| = m \geq 0$. If $m < i$, then by Corollary 3.3.17, $d(A, B) = \lceil \frac{k-m}{k-i} \rceil \geq 2$, and if $m > i$, then by Lemma 3.3.13, $d(A, B) = 2$. As m increases, the value of the function $\lceil \frac{k-m}{k-i} \rceil$ decreases. Hence the diameter of $\Gamma_{n,k,i}$ is the value of this function at $m = 0$, i.e. $\lceil \frac{k}{k-i} \rceil$. $\square$

3.4 Action of S_n on $I^{(k,l)}$

In this section we prove Theorems 3.2.5(2), 3.2.6(2) and 3.2.8(2). To do this, we will need Theorem 3.3.1(2) as well as the following results, which we shall also prove in this section.

Recall that for an $l \times l$ integer matrix M whose row and columns sums are k and for which $[M] = [M^T]$, the graph $\Gamma_{[M]}$ is the graph whose vertices are the kl -partitions of $\{1, \dots, kl\}$ and edges are $\{A, B\}$ where $I_{AB} \in [M]$.

Theorem 3.4.1. *Let $G := S_n$ or A_n and $\Omega := I^{(k,l)}$, where $n = kl$ with $k > 1$ and $l > 1$. Then $\text{diam}_O(G, \Omega) \geq \frac{l}{2} \lfloor \frac{k}{2} \rfloor$.*

Theorem 3.4.2. *Suppose $n = 2k$ with $k > 1$. For $i \in \{1, \dots, \lfloor k/2 \rfloor\}$, define*

$$M_i := \begin{pmatrix} i & k-i \\ k-i & i \end{pmatrix}.$$

1. For $k = 2, 3$, $\text{diam}(\Gamma_{[M_1]}) = 1$;

2. For $k \geq 4$,

(a) $\text{diam}(\Gamma_{[M_i]}) = 2$ if and only if $\frac{k-1}{4} \leq i \leq \frac{k}{2}$;

(b) if $\text{diam}(\Gamma_{[M_i]}) \neq 2$, then $\text{diam}(\Gamma_{[M_i]}) = \lceil \frac{k-1}{2i} \rceil$.

To prove Theorem 3.4.1, we will prove the existence of an orbital graph whose diameter is at least $\frac{l}{2} \lfloor \frac{k}{2} \rfloor$. We now define and analyse one such orbital graph.

Definition 3.4.3. Suppose $n = kl$, where $k, l > 1$. We define the $l \times l$ matrix

$$M_{kl} := \left(\begin{array}{c|cc} kI_{l-2} & 0 & 0 \\ \hline 0 & 1 & k-1 \\ 0 & k-1 & 1 \end{array} \right)$$

Remark 3.4.4. Observe that if $A, B \in V(\Gamma_{[M_{kl}]})$ are adjacent, then there exists a transposition in S_{kl} mapping A to B (where we are considering the natural action of S_{kl} on (k, l) -partitions). Hence every path between A and B can be represented by a sequence of transpositions and the number of transpositions is the length of the path. For a path P between A and B , we will use σ_P to denote the product of the corresponding sequence of transpositions.

Henceforth, for a permutation $\sigma \in S_n$, we will denote by $\text{supp}(\sigma)$, the support of σ , i.e. the set $\{x \in \{1, \dots, n\} : x^\sigma \neq x\}$ (again, we are considering the natural action of S_n on $\{1, \dots, n\}$ here).

Proposition 3.4.5. *For $k, l > 1$, we have $\text{diam}(\Gamma_{[M_{kl}]}) \geq \frac{l}{2} \lfloor \frac{k}{2} \rfloor$.*

Proof. Let A and B be two (k, l) -partitions such that

$$I_{AB} \sim \begin{pmatrix} \lfloor \frac{k}{2} \rfloor & \lceil \frac{k}{2} \rceil & 0 & \dots & 0 & 0 \\ 0 & \lfloor \frac{k}{2} \rfloor & \lceil \frac{k}{2} \rceil & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & \lfloor \frac{k}{2} \rfloor & \lceil \frac{k}{2} \rceil \\ \lceil \frac{k}{2} \rceil & 0 & \dots & \dots & 0 & \lfloor \frac{k}{2} \rfloor \end{pmatrix}. \quad (3.12)$$

Write $A = A_1 | \dots | A_l$ and $B = B_1 | \dots | B_l$. Let $r := d(A, B)$ and let P be a path of length r between A and B . Then σ_P maps A to B and for each $i \in \{1, \dots, l\}$ there exists $j \in \{1, \dots, l\}$ such that σ_P maps A_i to B_j . Now $|A_i \cap B_j| \leq \lceil \frac{k}{2} \rceil$ and hence σ_P moves at least $k - \lceil \frac{k}{2} \rceil = \lfloor \frac{k}{2} \rfloor$ elements from each A_i . Therefore $|\text{supp}(\sigma_P)|$ is at least $l \lfloor \frac{k}{2} \rfloor$. Any permutation whose support is at least x cannot be expressed as a product of fewer than $x/2$ transpositions. Therefore, σ_P is a product of at least $\frac{l}{2} \lfloor \frac{k}{2} \rfloor$ transpositions. By Remark 3.4.4, we have that r is greater than or equal to the minimal length of a factorisation of σ_P by transpositions, and thus $r \geq \frac{l}{2} \lfloor \frac{k}{2} \rfloor$, from which the result follows. $\square$

Proof of Theorem 3.4.1. If $(k, l) = (2, 2)$, then $\text{diam}_O(G, I^{(k,l)}) \geq 1 = \frac{l}{2} \lfloor \frac{k}{2} \rfloor$. Suppose $(k, l) \neq (2, 2)$. Then $\Delta_{[M_{kl}]}$ is an orbital of $(S_{kl}, I^{(k,l)})$, and we claim that it is also an orbital of $(A_{kl}, I^{(k,l)})$. Indeed, by Proposition 2.1.5 either $\Delta_{[M_{kl}]}$ remains an orbital of $(A_n, I^{(k,l)})$ or splits into two orbitals. We will show that the former holds by showing that A_{kl} is transitive on $\Delta_{[M_{kl}]}$.

Let (A, B) and (C, D) be two elements of $\Delta_{[M_{kl}]}$, and write $C = C_1 | \dots | C_l$ and $D = D_1 | \dots | D_l$. Since S_{kl} is transitive on $\Delta_{[M_{kl}]}$, there exists $g \in S_{kl}$ such that $(A, B)^g = (C, D)$. Suppose $g \in S_{kl} \setminus A_{kl}$. Now $I_{CD} \sim M_{kl}$ implies that there exist i, j such that $|C_i \cap D_j| \geq 2$. Pick two distinct elements $a, b \in C_i \cap D_j$ and let $h := g(ab)$. Then $h \in A_{kl}$ and $(A, B)^h = (C, D)$. This proves the claim and thus $\Gamma_{[M_{kl}]}$ is also an orbital graph of $(A_{kl}, I^{(k,l)})$. Finally $\text{diam}_O(G, I^{(k,l)}) \geq \text{diam}(\Gamma_{[M_{kl}]}) \geq \frac{l}{2} \lfloor \frac{k}{2} \rfloor$ by Proposition 3.4.5. $\square$

We now use Theorem 3.4.1 to prove Theorem 3.2.5(2).

Proof of Theorem 3.2.5(2). Suppose $\text{diam}_O(G, \Omega) \leq c$. If $(k, l) \neq (2, 2)$, then the proof of Theorem 3.4.1 shows that $\Gamma_{[M_{kl}]}$ is an orbital graph of (G, Ω) . Hence in particular, we have $\text{diam}(\Gamma_{[M_{kl}]}) \leq c$. Thus by Theorem 3.4.1, we have

$$\frac{l}{2} \left\lfloor \frac{k}{2} \right\rfloor \leq c. \quad (3.13)$$

Note that (3.13) also holds for $(k, l) = (2, 2)$. Now since $\lfloor \frac{k}{2} \rfloor \geq 1$, (3.13) implies $l \leq 2c$, and since $l \geq 2$ it also implies $k \leq 2c + 1$, and hence $n = kl \leq 2c(2c + 1)$. $\square$

We believe that the lower bound in Proposition 3.4.5 (and hence also the lower bound in Theorem 3.4.1) can be improved. To be precise, we conjecture the following.

Conjecture 3.4.6. *For $k, l > 1$, we have $\text{diam}(\Gamma_{[M_{kl}]}) \geq \lfloor \frac{k}{2} \rfloor (l - 1)$.*

The $l = 3$ case of Conjecture 3.4.6 is proved as Proposition 3.4.8 (see below). In general, if A and B are as in the proof of Proposition 3.4.5, then it seems that a shortest path between A and B can be obtained by fixing $\lfloor \frac{k}{2} \rfloor$ elements from each A_i and permuting the rest of the elements in $\lfloor \frac{k}{2} \rfloor$ cycles each of length l . Note that verification of the conjecture would allow one to prove results like Theorem 3.2.6(2) for values higher than 5; to prove the converse implication in the result, we use a computer which has limitations

as the values of k and l become large, but the improved lower bound would reduce the number of cases which need to be dealt with using a computer.

We now work towards proving Theorem 3.2.6(2).

Proposition 3.4.7. *Let $G := S_n$ or A_n and $\Omega := I^{(k,l)}$, where $n = kl$, $k > 1$, $l > 1$, and suppose that (k, l) is not in Table 3.8. Then $\text{diam}_O(G, \Omega) \geq 6$.*

l	2	3	4	5	6, 7, 8, 9, 10
k	≤ 11	≤ 7	≤ 5	≤ 5	≤ 3

Table 3.8: Possible pairs (k, l) with $\text{diam}_O(G, I^{(k,l)}) \leq 5$

Proof. It suffices to show that if $\text{diam}_O(G, \Omega) \leq 5$, then (k, l) is in Table 3.8. Suppose $\text{diam}_O(G, \Omega) \leq 5$. Then by Theorem 3.2.5(2) we must have $l \leq 10$. We obtain the values for k by using (3.13) with each $l \leq 10$ and $c = 5$. $\square$

In order to prove Theorem 3.2.6(2), for each pair (k, l) in Table 3.8, we must either determine that the diameters of all orbital graphs are bounded above by 5 or find an orbital graph of diameter greater than 5, for $(S_{kl}, I^{(k,l)})$ and $(A_{kl}, I^{(k,l)})$. To do this, for most cases of (k, l) we shall use one of two computer programs. However, these programs turn out not to be so efficient for large values of $n = kl$; to deal with these cases, we prove the following results. Henceforth we use the notation $A \sqcup B$ to mean the disjoint union of the two sets A and B .

For $l = 3$, we prove the following.

Proposition 3.4.8. *For all $k \geq 2$, we have $\text{diam}(\Gamma_{[M_{k3}]}) \geq 2 \lfloor \frac{k}{2} \rfloor$.*

Proof. Let $A = A_1|A_2|A_3$ and $B = B_1|B_2|B_3$ be two $(k, 3)$ -partitions with

$$I_{AB} = \begin{pmatrix} \lfloor \frac{k}{2} \rfloor & 0 & \lceil \frac{k}{2} \rceil \\ \lceil \frac{k}{2} \rceil & \lfloor \frac{k}{2} \rfloor & 0 \\ 0 & \lceil \frac{k}{2} \rceil & \lfloor \frac{k}{2} \rfloor \end{pmatrix}.$$

Let $r := d(A, B)$ and suppose that P is a path of length r between A and B . As in the proof of Proposition 3.4.5, σ_P must move at least $\lfloor \frac{k}{2} \rfloor$ elements from each A_i . If there exists i such that σ_P moves all k elements from A_i , then σ_P moves at least $k + 2 \lfloor \frac{k}{2} \rfloor$ elements in total, and hence $r \geq \lceil \frac{k}{2} + \lfloor \frac{k}{2} \rfloor \rceil = k \geq 2 \lfloor \frac{k}{2} \rfloor$. Now assume that σ_P fixes at least one element from each A_i . Define $X_1 := A_1 \cap B_1$, $Y_1 := A_2 \cap B_2$ and $Z_1 := A_3 \cap B_3$, and let X_2 , Y_2 and Z_2 be their complements in A_1 , A_2 and A_3 respectively. Then the following information can be read off I_{AB} :

$$|X_1| = |Y_1| = |Z_1| = \left\lfloor \frac{k}{2} \right\rfloor, |X_2| = |Y_2| = |Z_2| = \left\lceil \frac{k}{2} \right\rceil,$$

$$A_1 = X_1 \sqcup X_2, A_2 = Y_1 \sqcup Y_2, A_3 = Z_1 \sqcup Z_2,$$

$$B_1 = X_1 \sqcup Y_2, B_2 = Y_1 \sqcup Z_2, B_3 = Z_1 \sqcup X_2.$$

Now either $A_1^{\sigma_P} = B_1$ or $A_1^{\sigma_P} = B_3$. Suppose $A_1^{\sigma_P} = B_1$. Then $A_i^{\sigma_P} = B_i$ for all i . Now if $\alpha \in X_2$ and $\beta := \alpha^{\sigma_P}$, then $\beta \in X_1 \sqcup Y_2$, so $\beta \neq \alpha$. Also, if $\beta \in Y_2$ then $\beta^{\sigma_P} \in Y_1 \sqcup Z_2$, so $\beta^{\sigma_P} \neq \alpha$, and if $\beta \in X_1$, then $\beta^{\sigma_P} \in X_1 \sqcup Y_2$, so again $\beta^{\sigma_P} \neq \alpha$. Hence in the cycle decomposition of σ_P , α is contained in a cycle of length at least 3. Repeating similar arguments we see that the same holds if $\alpha \in Y_2$ or $\alpha \in Z_2$. Now r is greater than or equal to the minimal length of a factorisation of σ_P by transpositions. Using the fact that the minimal length of a factorisation of a permutation σ by transpositions is $|\text{supp}(\sigma)| - c_\sigma$, where c_σ is the number of non-trivial cycles in the disjoint cycle decomposition of σ , we have $r \geq |\text{supp}(\sigma_P)| - c_{\sigma_P}$. Suppose that there are s disjoint cycles of length at least 3 in the disjoint cycle decomposition of σ_P . Let $J \subseteq \{1, \dots, n\}$ be the union of the supports of these cycles. Then $|\text{supp}(\sigma_P)| - c_{\sigma_P} \geq |J| - s$ (this is because $c_{\sigma_P} - s$ is the number of 2-cycles in the cycle decomposition of σ_P , whereas $|\text{supp}(\sigma_P)| - |J|$ is twice this number). Furthermore, $s \leq \frac{1}{3}|J|$ and hence $r \geq \frac{2}{3}|J|$. On the other hand, the preceding discussion implies $|J| \geq |X_2 \cup Y_2 \cup Z_2| = 3 \lceil \frac{k}{2} \rceil$. Combining the

two we obtain $r \geq 2 \lceil \frac{k}{2} \rceil \geq 2 \lfloor \frac{k}{2} \rfloor$. Now suppose $A_1^{\sigma_P} = B_3$. Then $A_2^{\sigma_P} = B_1$ and $A_3^{\sigma_P} = B_2$. Repeating similar arguments to the above we can see that every element of $X_1 \cup Y_1 \cup Z_1$ must be contained in a cycle of length at least 3, and so as above we have that

$$r \geq \frac{2}{3} 3 \left\lfloor \frac{k}{2} \right\rfloor = 2 \left\lfloor \frac{k}{2} \right\rfloor.$$

Therefore $d(A, B) \geq 2 \lfloor \frac{k}{2} \rfloor$, from which the result follows. $\square$

For $k = 3$, we have the following result.

Proposition 3.4.9. *For all $l \geq 4$, we have $\text{diam}(\Gamma_{[M_{3l}]}) \geq \lceil \frac{l}{2} \rceil + 1$.*

Proof. Let A and B be two $(3, l)$ -partitions with

$$I_{AB} = \begin{pmatrix} 1 & 2 & 0 & \dots & 0 \\ 0 & 1 & 2 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 & 2 \\ 2 & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

as in (3.12). By the proof of Proposition 3.4.5, $d(A, B) \geq \lceil \frac{l}{2} \rceil$. We will prove the result by showing that $d(A, B) > \lceil \frac{l}{2} \rceil$. Assume by contradiction that P is a path of length $\lceil \frac{l}{2} \rceil$ between A and B . Write $\sigma_P = a_1 \cdots a_{\lceil \frac{l}{2} \rceil}$, where each a_i is a transposition, and write $A = A_1 | \dots | A_l$. As in the proof of Proposition 3.4.5, σ_P moves at least one element from each A_i . It follows that if l is even, then $|\text{supp}(\sigma_P)| = l$ and if l is odd, then $|\text{supp}(\sigma_P)| \in \{l, l+1\}$. In all cases $\text{supp}(\sigma_P) = \cup_{i=1}^{\lceil \frac{l}{2} \rceil} \text{supp}(a_i)$, and now a careful analysis, whose details are left to the reader, shows that in all cases there exists $1 \leq i \leq \lceil \frac{l}{2} \rceil$ and $1 \leq r \neq s \leq l$ such that $a_i = (xy)$ for some $x \in A_r$ and $y \in A_s$;

moreover, the supports of a_i and a_j are disjoint for all $1 \leq j \leq \lceil \frac{l}{2} \rceil$, $j \neq i$, and $|\text{supp}(\sigma_P) \cap A_r| = |\text{supp}(\sigma_P) \cap A_s| = 1$. In particular, a_i commutes with every other transposition a_j and so we can write $\sigma_P = a_i \sigma'_P$ where $\sigma'_P := a_1 \cdots a_{i-1} a_{i+1} \cdots a_{\lceil \frac{l}{2} \rceil}$. Thus σ_P maps A_r to $(A_r \setminus \{x\}) \cup \{y\}$ and A_s to $(A_s \setminus \{y\}) \cup \{x\}$. Therefore $I_{AB} \sim N$, where N is the $l \times l$ matrix

$$\begin{pmatrix} M & 0 \\ 0 & X \end{pmatrix},$$

with

$$M := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

and X a $(l-2) \times (l-2)$ matrix. Thus there exist permutation matrices P and Q such that $P^{-1}I_{AB} = NQ$. Recall that multiplication by P^{-1} on the left permutes the rows of I_{AB} , and multiplication by Q on the right permutes the columns of N . Now the entries of $P^{-1}I_{AB} = NQ$ take values from the set $\{0, 1, 2\}$. Firstly, suppose $(NQ)_{11} = 2$. Then the first and second rows of $P^{-1}I_{AB}$ must be $(2, 0, \dots, 0, 1)$ and $(1, 2, 0, \dots, 0)$, respectively. This implies that $(NQ)_{12} = 0$ and $(NQ)_{22} = 2$, which is not possible since N does not contain a column of the form $(0, 2, \dots)^T$. Now suppose that $(NQ)_{11} = 1$. Then the first and second rows of $P^{-1}I_{AB}$ must be $(1, 2, 0, \dots, 0)$ and $(2, 0, \dots, 0, 1)$ respectively. This implies that $(NQ)_{12} = 2$ and $(NQ)_{22} = 0$, which is again not possible. Finally suppose that $(NQ)_{11} = 0$. Then $(NQ)_{21} = 0$ and there exist $i \in \{2, \dots, l\}$ such that $(NQ)_{1i} = 1$ and $(NQ)_{2i} = 2$. However this is a contradiction since the matrix I_{AB} has the property that if $(I_{AB})_{r1} = (I_{AB})_{s1} = 0$ and $(I_{AB})_{rt} = 1$, then $(I_{AB})_{st} = 0$, where $t \in \{2, \dots, l\}$. Therefore $d(A, B) \geq \lceil \frac{l}{2} \rceil + 1$. $\square$

We also have a small improvement to the lower bound in Proposition 3.4.5 which is obtained as follows.

Proposition 3.4.10. *Let $A, B \in V(\Gamma_{[M_{kl}]})$ with I_{AB} as in (3.12). If P is a path between A and B and $\sigma_P \in S_{kl}$ moves exactly $l \lfloor \frac{k}{2} \rfloor$ points from A , then $d(A, B) \geq \lfloor \frac{k}{2} \rfloor (l - 1)$, and hence $\text{diam}(\Gamma_{[M_{kl}]}) \geq \lfloor \frac{k}{2} \rfloor (l - 1)$.*

Proof. Write $A = A_1 | \dots | A_l$ and $B = B_1 | \dots | B_l$. Since I_{AB} is given by (3.12) we can write $A_i = X_i \sqcup Y_i$ for all $i \in \{1, \dots, l\}$, where $|X_i| = \lfloor \frac{k}{2} \rfloor$, $B_1 = X_1 \sqcup Y_l$, and $B_i = X_i \sqcup Y_{i-1}$ for all $i \in \{2, \dots, l\}$. As in the proof of Proposition 3.4.5, σ_P moves at least $\lfloor \frac{k}{2} \rfloor$ elements from each A_i . Hence by the assumption exactly $\lfloor \frac{k}{2} \rfloor$ elements are moved from each A_i . Therefore $A_i^{\sigma_P} = B_i$, for all i . In particular, $X_i^{\sigma_P} = X_{i+1}$, for $i \in \{1, \dots, l-1\}$, and $X_l^{\sigma_P} = X_1$. Hence writing $\sigma_P = C_1 \cdots C_r$, where the C_i are non-trivial disjoint cycles, we conclude that each C_i has length which is a multiple of l , say $t_i l$, and $r \leq \lfloor \frac{k}{2} \rfloor$. Then $\sum_{i=1}^r t_i l = \lfloor \frac{k}{2} \rfloor l$ and σ_P cannot be expressed as a product of fewer than

$$\sum_{i=1}^r (t_i l - 1) = \left\lfloor \frac{k}{2} \right\rfloor l - r$$

transpositions. The expression on the right hand side is minimal when $r = \lfloor \frac{k}{2} \rfloor$ and hence $d(A, B) \geq \lfloor \frac{k}{2} \rfloor (l - 1)$. $\square$

Corollary 3.4.11. *For all $k, l \geq 2$, we have*

$$\text{diam}(\Gamma_{[M_{kl}]}) \geq \min \left\{ \left\lceil \frac{l}{2} \left\lfloor \frac{k}{2} \right\rfloor + \frac{1}{2} \right\rceil, \left\lfloor \frac{k}{2} \right\rfloor (l - 1) \right\}.$$

In particular, for $k \geq 2$ and $l \geq 3$, we have $\text{diam}(\Gamma_{[M_{kl}]}) \geq \lceil \frac{l}{2} \lfloor \frac{k}{2} \rfloor + \frac{1}{2} \rceil$.

Proof. Let $A, B \in V(\Gamma_{[M_{kl}]})$ with I_{AB} as in (3.12) and let P be a path between A and B . Then σ_P moves at least $l \lfloor \frac{k}{2} \rfloor$ points from A . Now if σ_P moves exactly $l \lfloor \frac{k}{2} \rfloor$ points then $\text{diam}(\Gamma_{[M_{kl}]}) \geq \lfloor \frac{k}{2} \rfloor (l - 1)$ by Proposition 3.4.10. Otherwise σ_P moves at least $l \lfloor \frac{k}{2} \rfloor + 1$ points and hence cannot be expressed as a product of fewer than $\frac{l \lfloor \frac{k}{2} \rfloor + 1}{2}$ transpositions. Thus

$\text{diam}(\Gamma_{[M_{kl}]}) \geq d(A, B) \geq \lceil \frac{l}{2} \lfloor \frac{k}{2} \rfloor + \frac{1}{2} \rceil$. Finally, one can easily check that for $l \geq 3$, $\lceil \frac{l}{2} \lfloor \frac{k}{2} \rfloor + \frac{1}{2} \rceil \leq \lfloor \frac{k}{2} \rfloor (l-1)$. $\square$

For the case $l = 2$, we find the diameters of all orbital graphs of $(S_{kl}, I^{(k,l)})$ as stated in Theorem 3.4.2. Recall that for $l = 2$ the orbital graphs are $\Gamma_{[M_i]}$, where $i \in \{1, \dots, \lfloor k/2 \rfloor\}$ and

$$M_i = \begin{pmatrix} i & k-i \\ k-i & i \end{pmatrix}.$$

Note that the matrix M_i is determined by $(M_i)_{11}$ and if $A, B \in V(\Gamma_{[M_i]})$, then the matrix I_{AB} is determined by $(I_{AB})_{11}$. In order to prove Theorem 3.4.2 we will need to prove the following criterion which relates distances in the graphs $\Gamma_{[M_i]}$ to distances in the graphs $\Gamma_{2k,k,i}$ from Section 3.3. In what follows, for a k -subset X of $I = \{1, \dots, 2k\}$, we will use the notation X^c to refer to $I \setminus X$.

Lemma 3.4.12. *Let $i \in \{1, \dots, \lfloor k/2 \rfloor\}$, $r \geq 2$, and $A, B \in V(\Gamma_{[M_i]})$ where $A = A_1|A_2$, $B = B_1|B_2$ and $(M_i)_{11} := i$. Suppose $d_{\Gamma_{[M_i]}}(A, B) \geq r$. Then $d_{\Gamma_{[M_i]}}(A, B) = r$ if and only if there exist $l, m \in \{1, 2\}$ such that $d_{\Gamma_{2k,k,i}}(A_l, B_m) = r$. In particular, we have $\text{diam}(\Gamma_{[M_i]}) \geq r$ if and only if $\text{diam}(\Gamma_{2k,k,i}) \geq r$.*

Proof. Suppose $d_{\Gamma_{[M_i]}}(A, B) = r$ and let $A - C_1 - \dots - C_{r-1} - B$ be a shortest path, where $C_i := X_i|Y_i$. Then there exist $\{l, m\} \in \{1, 2\}$, and $Z_i \in \{X_i, Y_i\}$ for $i \in \{1, \dots, r-1\}$, such that $|A_l \cap Z_1| = i$, $|Z_i \cap Z_{i+1}| = i$ for $i \in \{1, \dots, r-2\}$, and $|Z_{r-1} \cap B_m| = i$. Hence $A_l - Z_1 - \dots - Z_{r-1} - B_m$ is a path of length r in $\Gamma_{2k,k,i}$. If $d_{\Gamma_{2k,k,i}}(A_l, B_m) =: t < r$ and $A_l - D_1 - \dots - D_{t-1} - B_m$ is a shortest path, then

$$A = A_l|A_l^c - D_1|D_1^c - \dots - D_{t-1}|D_{t-1}^c - B_m|B_m^c = B$$

is a path of length t in $\Gamma_{[M_i]}$, contradicting the fact that $d_{\Gamma_{[M_i]}}(A, B) = r > t$.

Hence $d_{\Gamma_{2k,k,i}}(A_l, B_m) = r$. Conversely, suppose there exist $l, m \in \{1, 2\}$ such that $d_{\Gamma_{2k,k,i}}(A_l, B_m) = r$. Let $A_l - X_1 - \cdots - X_{r-1} - B_m$ be a shortest path in $\Gamma_{2k,k,i}$. Then

$$A = A_l | A_l^c - X_1 | X_1^c - \cdots - X_{r-1} | X_{r-1}^c - B_m | B_m^c = B$$

is a path of length r in $\Gamma_{[M_i]}$, and since $d_{\Gamma_{[M_i]}}(A, B) \geq r$, we have that $d_{\Gamma_{[M_i]}}(A, B) = r$. $\square$

The following lemma follows directly from Lemmas 3.3.4 and 3.3.6.

Lemma 3.4.13. *Let $i \in \{1, \dots, \lfloor k/2 \rfloor\}$ and let $A, B \in V(\Gamma_{2k,k,i})$ where $m := |A \cap B| \neq i$. Suppose $d := \text{diam}(\Gamma_{2k,k,i}) \geq 2$. Then*

$$d(A, B) = 2 \Leftrightarrow m \geq k - 2i.$$

In particular, if $2i \geq k$, then $d(A, B) = 2$. Now suppose $d \geq 3$ and let $v \in \{3, \dots, d\}$. If $(2v - 1)i < k$, then

$$\begin{aligned} d(A, B) = v &\Leftrightarrow k - vi \leq m < k - (v - 2)i, & v \text{ even} \\ d(A, B) = v &\Leftrightarrow (v - 2)i < m \leq vi, & v \text{ odd}, \end{aligned}$$

and if $(2v - 1)i \geq k$, then

$$d(A, B) = v \Leftrightarrow (v - 1)i < m < k - (v - 2)i, \quad v \text{ even}$$

$$d(A, B) = v \Leftrightarrow (v - 2)i < m < k - (v - 1)i, \quad v \text{ odd}.$$

Proof of Theorem 3.4.2(1) and (2a). It is straightforward to verify that for $k < 4$, all orbital graphs have diameter 1. Suppose $k \geq 4$ and let $A, B \in V(\Gamma_{[M_i]})$ with $(I_{AB})_{11} := j$, where $j \in \{1, \dots, \lfloor k/2 \rfloor\}$ and $j \neq i, k - i$. Then $d_{\Gamma_{[M_i]}}(A, B) \geq 2$ and by Lemma 3.4.12, $d_{\Gamma_{[M_i]}}(A, B) = 2$ if and only if there

exist $l, m \in \{1, 2\}$ such that $d_{\Gamma_{2k,k,i}}(A_l, B_m) = 2$. Hence by Lemma 3.4.13,

$$d_{\Gamma_{[M_i]}}(A, B) = 2 \Leftrightarrow \text{either } j \geq k - 2i \text{ or } j \leq 2i. \quad (3.14)$$

Therefore $\text{diam}(\Gamma_{[M_i]}) = 2$ if and only if $2i \geq k - 2i - 1$, i.e. $i \geq \frac{k-1}{4}$. $\square$

Lemma 3.4.14. *Let $i \in \{1, \dots, \lfloor k/2 \rfloor\}$ and let $A, B \in V(\Gamma_{[M_i]})$ where $(I_{AB})_{11} := j$ for some $j \in \{1, \dots, \lfloor k/2 \rfloor\}$ and $j \neq i, k - i$. Suppose that $d_{\Gamma_{[M_i]}}(A, B) \geq 3$. If $5i < k$, then*

$$d_{\Gamma_{[M_i]}}(A, B) = 3 \Leftrightarrow \text{either } 2i < j \leq 3i \text{ or } k - 3i \leq j < k - 2i, \quad (3.15)$$

and if $5i \geq k$, then

$$d_{\Gamma_{[M_i]}}(A, B) = 3 \Leftrightarrow 2i < j < k - 2i. \quad (3.16)$$

Proof. Note that since $d_{\Gamma_{[M_i]}}(A, B) \geq 3$, (3.14) implies $2i < j < k - 2i$. We detail the proof for the case where $5i < k$; the proof for the case where $5i \geq k$, can be done analogously. Suppose $5i < k$. If $d_{\Gamma_{[M_i]}}(A, B) = 3$, then by Lemma 3.4.12 there exist k -subsets A_1, B_1 with $|A_1 \cap B_1| = j$ or $k - j$ such that $d_{\Gamma_{2k,k,i}}(A_1, B_1) = 3$. Then by Lemma 3.4.13 we have that either $i < j \leq 3i$ or $k - 3i \leq j < k - i$. Combining these with $2i < j < k - 2i$ gives the result in one direction. The converse implication follows directly by using Lemmas 3.4.12 and 3.4.13. $\square$

Lemma 3.4.15. *Let $t \geq 2$ and suppose $\text{diam}(\Gamma_{[M_i]}) \geq t + 1$. If $t = 2$, then $2i < k$, and if $t \geq 3$, then $(2t - 1)i < k$.*

Proof. Note that we have $2i \leq k$. If $2i = k$, then $\text{diam}(\Gamma_{[M_i]}) = 2$ by Theorem 3.4.2(2a), and hence the result for $t = 2$. If $t \geq 3$, then $\text{diam}(\Gamma_{2k,k,i}) \geq t + 1$ by Lemma 3.4.12, and the result follows from Lemma 3.3.9. $\square$

Proposition 3.4.16. *Let $i \in \{1, \dots, \lfloor k/2 \rfloor\}$. Then*

$$\text{diam}(\Gamma_{[M_i]}) = 3 \Leftrightarrow \frac{k-1}{6} \leq i < \frac{k-1}{4}.$$

Proof. Suppose $\text{diam}(\Gamma_{[M_i]}) = 3$. Then $\text{diam}(\Gamma_{[M_i]}) > 2$, and so by Theorem 3.4.2(2a), we must have $i < \frac{k-1}{4}$. Then using (3.14) and Lemma 3.4.14, we see that $3i \geq k - 3i - 1$, i.e. $i \geq \frac{k-1}{6}$. Conversely suppose $\frac{k-1}{6} \leq i < \frac{k-1}{4}$. Then $\text{diam}(\Gamma_{[M_i]}) \geq 3$ by Theorem 3.4.2(2a). Now using (3.14) and Lemma 3.4.14, and the fact that $i \geq \frac{k-1}{6}$, we see that for all $A, B \in V(\Gamma_{[M_i]})$ with $d(A, B) > 2$, we must have $d(A, B) = 3$, and thus $\text{diam}(\Gamma_{[M_i]}) = 3$. $\square$

We now prove a result generalising (3.14), (3.15) and (3.16).

Lemma 3.4.17. *Let $r \geq 3$ and $A, B \in V(\Gamma_{[M_i]})$ with $(I_{AB})_{11} =: j$, where $j \in \{1, \dots, k/2\}$ and $j \neq i, k - i$. Suppose $d_{\Gamma_{[M_i]}}(A, B) \geq r$.*

1. *If $(2r - 1)i < k$, then $d_{\Gamma_{[M_i]}}(A, B) = r$ if and only if either $k - ri \leq j < k - (r - 1)i$ or $(r - 1)i < j \leq ri$.*
2. *If $(2r - 1)i \geq k$, then $d_{\Gamma_{[M_i]}}(A, B) = r$ if and only if $(r - 1)i < j < k - (r - 1)i$.*

Proof. We proceed by induction on r . The base case $r = 3$ has been done in Lemma 3.4.14. Now suppose $d_{\Gamma_{[M_i]}}(A, B) \geq r \geq 4$ and that the result holds for all $s < r$. Note that (3.14) determines the pairs of vertices for which the distance is 2. Moreover, since $d_{\Gamma_{[M_i]}}(A, B) \geq 4$, using Lemma 3.4.15 with $t = 3$, we have $5i < k$ and thus (3.15) determines the pairs of vertices for which the distance is 3. Now, for $s < r$ since $d_{\Gamma_{[M_i]}}(A, B) \geq r \geq s + 1$, by Lemma 3.4.15, we have $(2s - 1)i < k$ and thus using the inductive hypothesis, we can determine the pairs of vertices for which the distance is s . Combining the above, we obtain that

$$d_{\Gamma_{[M_i]}}(A, B) \geq r \Leftrightarrow (r - 1)i < j < k - (r - 1)i. \quad (3.17)$$

For j as in (3.17), using Lemmas 3.4.12 and 3.4.13, if $(2r - 1)i < k$, we have

$$d_{\Gamma_{[M_i]}}(A, B) = r \Leftrightarrow \text{either } k - ri \leq j < k - (r - 2)i \text{ or } (r - 2)i < j \leq ri,$$

and if $(2r - 1)i \geq k$, then

$$\begin{aligned} d_{\Gamma_{[M_i]}}(A, B) = r \Leftrightarrow \\ \text{either } (r - 1)i < j < k - (r - 2)i \text{ or } (r - 2)i < j < k - (r - 1)i. \end{aligned}$$

We obtain the result by combining the inequalities above with (3.17). $\square$

The next result is a direct consequence of the proof of Lemma 3.4.17.

Lemma 3.4.18. *Let $r \geq 3$ and $A, B \in V(\Gamma_{[M_i]})$ with $(I_{AB})_{11} := j$, where $j \in \{1, \dots, k/2\}$ and $j \neq i, k - i$. If $\text{diam}(\Gamma_{[M_i]}) \geq r$, then*

$$d_{\Gamma_{[M_i]}}(A, B) \geq r \Leftrightarrow (r - 1)i < j < k - (r - 1)i.$$

We now prove Theorem 3.4.2(2b).

Proof of Theorem 3.4.2(2b). Suppose $\text{diam}(\Gamma_{[M_i]}) \neq 2$. It suffices to show that for $r \geq 3$,

$$\text{diam}(\Gamma_{[M_i]}) = r \Leftrightarrow \frac{k - 1}{2r} \leq i < \frac{k - 1}{2r - 2}.$$

We proceed by induction on r . The base case $r = 3$ is done in Proposition 3.4.16. Now let $r \geq 4$ and suppose for the inductive hypothesis that

$$\text{diam}(\Gamma_{[M_i]}) = s \Leftrightarrow \frac{k - 1}{2s} \leq i < \frac{k - 1}{2s - 2}, \quad (3.18)$$

for all $s \in \{3, \dots, r - 1\}$. Suppose that $\text{diam}(\Gamma_{[M_i]}) = r$. Then we have $\text{diam}(\Gamma_{[M_i]}) > r - 1$, and so by Theorem 3.4.2(2a) and (3.18), we must have $i < \frac{k-1}{2r-2}$. By Lemma 3.4.18 we have that for all $A, B \in V(\Gamma_{[M_i]})$ with

$(I_{AB})_{11} =: j$, where $j \in \{1, \dots, \lfloor k/2 \rfloor\}$ and $j \neq i, k - i$,

$$d_{\Gamma_{[M_i]}}(A, B) \geq r \Leftrightarrow (r - 1)i < j < k - (r - 1)i.$$

Now $\text{diam}(\Gamma_{[M_i]}) = r$ implies that for all $A, B \in V(\Gamma_{[M_i]})$ with $d(A, B) \geq r$, we must have $d(A, B) = r$. Using this and Lemma 3.4.17, we see that either $(2r - 1)i \geq k$, or $(2r - 1)i < k$ and $ri \geq k - ri - 1$. In either case, $i \geq \frac{k-1}{2r}$. Conversely, suppose $\frac{k-1}{2r} \leq i < \frac{k-1}{2r-2}$. Again by Theorem 3.4.2(2b) and (3.18), we have $\text{diam}(\Gamma_{[M_i]}) \geq r$. Then using Lemma 3.4.18, Lemma 3.4.17, and the fact that $i \geq \frac{k-1}{2r}$, we see that for all $A, B \in V(\Gamma_{[M_i]})$ with $d(A, B) \geq r$, we have $d(A, B) = r$, and thus $\text{diam}(\Gamma_{[M_i]}) = r$. $\square$

Proof of Theorem 3.2.6(2). Suppose $\text{diam}_O(G, \Omega) \leq 5$. By Proposition 3.4.7, the pair (k, l) must be in Table 3.8. For each such pair (k, l) , we now verify whether or not the converse holds. Suppose $l = 2$. If $k = 2$, then (S_{kl}, Ω) only has one orbital graph of diameter 1; by Lemma 3.4.22 (see below), this graph remains an orbital graph of (A_{kl}, Ω) . Thus the converse holds in this case. If $k \geq 3$, then using the same technique used in the proof of Theorem 3.4.1 to show that the orbital graph $\Gamma_{[M_{kl}]}$ remains an orbital graph of (A_{kl}, Ω) , one can show that the orbital graphs $\Gamma_{[M_i]}$ also remain orbital graphs of (A_{kl}, Ω) . Then Theorem 3.4.2 implies that the converse holds for $k \in \{3, \dots, 11\}$. Now using Proposition 3.4.8 (with $k = 6, 7$), Proposition 3.4.9 (with $l = 9, 10$), and Corollary 3.4.11 (with $(k, l) = (4, 5)$ and $(5, 5)$) we see that $\text{diam}(\Gamma_{[M_{kl}]} \geq 6$ for the pairs $(k, l) = (6, 3), (7, 3), (3, 9), (3, 10), (4, 5), (5, 5)$, and hence the converse does not hold for these pairs. For the remaining pairs from Table 3.8 we try to use the computer program $C_{\text{DIAM}}^G(k, l)$ (detailed in Sections 5.1 and 5.2 of Chapter 5) to output the diameters of all orbital graphs of $(G, I^{(k, l)})$. In the case where the attempt is successful, the output enables us to determine whether or not $\text{diam}_O(G, \Omega) \leq 5$. In some cases (namely $(k, l) = (5, 4), (3, 6), (3, 7), (3, 8), (2, 10)$) the attempt fails due to limitations of the computer program, described in Section 5.1; let (k, l) be

such as a case. Let $A, B \in \Gamma_{[M_{kl}]}$ with I_{AB} as in (3.12) and let σ be any permutation such that $A^\sigma = B$. Now any permutation mapping A to B is of the form $w\sigma$, where $w \in H_A \cong S_k \wr S_l$ ($H := S_{kl}$). For each permutation g mapping A to B , let T_g be the least number of transpositions g can be a product of. Then the minimum value of T_g amongst all g is a lower bound for the distance between A and B and hence a lower bound for the diameter of $\Gamma_{[M_{kl}]}$. We use the computer program $C_{\text{LOW}}(k, l, \sigma)$ (detailed in Section 5.3 of Chapter 5) to output this lower bound. For all inputs of (k, l) except $(3, 6)$, we obtain $\text{diam}(\Gamma_{[M_{kl}]}) \geq 6$, and thus the converse does not hold in these cases. For the case $(k, l) = (3, 6)$, we use $C_{\text{LOW}}(k, l, \sigma)$ but with σ such that $A^\sigma = B$ where

$$I_{AB} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

to again obtain $\text{diam}(\Gamma_{[M_{kl}]}) \geq 6$ for this case, i.e. the converse does not hold for this case either. Collating the results together, it turns out that the only pairs from Table 3.8 for which $\text{diam}_O(G, \Omega) \leq 5$, are the ones in the statement of the result, i.e. in Table 3.1. $\square$

Although the orbital diameters of $(S_{kl}, I^{(k,l)})$ tend to infinity as $n = kl$ does, there do exist infinite families of orbital graphs with small diameters. We will now present one infinite family of graphs of diameter 2 and prove Theorem 3.2.8(2). To do this we will need the following preliminary notions.

Definition 3.4.19. Let A be an $n \times n$ matrix with non-negative real entries.

1. Let $k \geq 1$ be an integer. We say that A is a *k-doubly stochastic* matrix if each row sum and each column sum is k . We say that A is *doubly stochastic* if A is 1-doubly stochastic.

2. A *diagonal* $D = (a_1, \dots, a_n)$ of A is a sequence of n entries of A such that no two entries lie in the same row or column of A . A diagonal D is called *positive* if $a_i > 0$ for all i .

Lemma 3.4.20 (Lemma 7.4.4 in [12]). *Every doubly stochastic matrix has a positive diagonal.*

Recall from Proposition 2.1.5 that since A_n is a subgroup of S_n of index 2, an orbital of $(S_{kl}, I^{(k,l)})$ either splits in $(A_{kl}, I^{(k,l)})$ or remains the same. Below we give a more specific criterion for determining which one of the previous two happens for a given orbital, and then use it with a particular orbital.

Proposition 3.4.21. *Let (G, X) and (H, X) be transitive permutation groups, where $G := S_n$ and $H := A_n$. Let $\Delta := y^{G_x}$ be a non-trivial suborbit of (G, X) . Then Δ remains a suborbit of (H, X) if and only if G_{xy} contains an odd permutation.*

Proof. By Proposition 2.1.5, either $|G_{xy}| = |H_{xy}|$ in which case the suborbit splits, or $|G_{xy}| = 2|H_{xy}|$ in which case the suborbit doesn't split. Now the former holds if and only if $G_{xy} = H_{xy}$ which is if and only if G_{xy} contains no odd permutation. Therefore, the latter holds if and only if G_{xy} contains an odd permutation. $\square$

Lemma 3.4.22. *Let $G := S_n$ and $H := A_n$, where $n = k^2$. Let $\Delta_{[M]}$ be the orbital of $(G, I^{(k,k)})$ where M is the $k \times k$ matrix with all entries equal to 1, and let $(\alpha, \beta) \in \Delta_{[M]}$. Then*

1. $G_{\alpha\beta} \cong S_k \times S_k$;
2. $G_{\alpha\beta} \leq H$ if and only if k is even, i.e. $\Delta_{[M]}$ splits in $(H, I^{(k,k)})$ if and only if k is even;
3. If k is even and $k/2$ is odd, then $\Delta_{[M]}$ splits into two orbitals of $(H, I^{(k,k)})$ which are paired with each other.

Proof. Write $\alpha = \alpha_1 | \dots | \alpha_k$ and $\beta = \beta_1 | \dots | \beta_k$, and $\alpha_i = \{\alpha_{i1}, \dots, \alpha_{ik}\}$. By relabelling the α_{ij} 's if necessary, we may write $\beta_i = \{\alpha_{1i}, \dots, \alpha_{ki}\}$.

We first prove part 1. For $\sigma \in S_k$, let g_σ denote the element of G_α which maps α_{ij} to $\alpha_{ij\sigma}$, and let h_σ denote the element of G_α which maps α_{ij} to $\alpha_{i\sigma j}$. Define $H_1 := \{g_\sigma : \sigma \in S_k\} \leq G_\alpha$ and $H_2 := \{h_\sigma : \sigma \in S_k\} \leq G_\alpha$. Now each g_σ and h_σ also stabilise β and thus $S_k \cong H_i \leq G_\beta$ for $i = 1, 2$. Furthermore, H_1 and H_2 commute and hence $S_k \times S_k \cong \langle H_1, H_2 \rangle \leq G_{\alpha\beta}$. In order to complete the proof of part 1, we will show that $|G_{\alpha\beta}| = (k!)^2$. By the Orbit-Stabiliser property, this is equivalent to showing that $|\beta^{G_\alpha}| = (k!)^{k-1}$. Now $\beta^{G_\alpha} = \{\gamma : (\alpha, \gamma) \in \Delta_{[M]}\}$ and thus $|\beta^{G_\alpha}|$ is the number of distinct (k, k) -partitions γ satisfying $I_{\alpha\gamma} = M$. This number can easily be seen to be $(k^k(k-1)^k \dots 2^k 1^k)/k! = (k!)^{k-1}$. This completes the proof of part 1.

We now prove part 2. Define $g := (\alpha_{11} \alpha_{21})(\alpha_{12} \alpha_{22}) \dots (\alpha_{1k} \alpha_{2k})$ and observe that $g \in G_{\alpha\beta}$. If k is odd, then $g \notin H$, i.e. $G_{\alpha\beta} \not\leq H$. Conversely, suppose k is even. Observe that if $\sigma \in S_k$ is a product of t transpositions, then g_σ will be a product of kt transpositions. Similarly, observe that if the cycle decomposition of $\sigma \in S_k$ has σ_i cycles of length i , then the cycle decomposition of h_σ will have $k\sigma_i$ cycles of length i . Therefore, if k is even, then $G_{\alpha\beta} = \langle H_1, H_2 \rangle \leq H$. Now by Proposition 3.4.21, the orbital $\Delta_{[M]}$ splits if and only if $G_{\alpha\beta} \leq H$, i.e. if and only if k is even.

We now prove part 3. Suppose k is even. By part 2, $\Delta_{[M]}$ splits in $(H, I^{(k,k)})$, into two orbitals, say Δ_1 and Δ_2 . These orbitals are interchanged by any odd permutation. By relabelling if necessary, we may assume that $(\alpha, \beta) \in \Delta_1$. In order to show that Δ_1 and Δ_2 are paired with each other, it suffices to show that there exists an odd permutation swapping α and β (since the existence of such a permutation implies $(\beta, \alpha) \in \Delta_2$). Indeed, the

permutation

$$\begin{aligned}
g := & (\alpha_{12} \alpha_{21}) \cdots (\alpha_{1k} \alpha_{k1}) \\
& (\alpha_{23} \alpha_{32}) \cdots (\alpha_{2k} \alpha_{k2}) \\
& \vdots \\
& (\alpha_{k-2,k-1} \alpha_{k-1,k-2}) (\alpha_{k-2,k} \alpha_{k,k-2}) \\
& (\alpha_{k-1,k} \alpha_{k,k-1})
\end{aligned}$$

swaps α and β and is a product of $k(k-1)/2$ transpositions which is odd if $k/2$ is odd. This proves part 3. $\square$

Proof of Theorem 3.2.8(2). By Lemma 3.4.22, if k is odd, or if k is even and $k/2$ is odd, then $\Gamma_{[M]}$ is an orbital graph of $(A_n, I^{(k,k)})$.

It remains to show that $\text{diam}(\Gamma_{[M]}) = 2$. Let $A, B \in V(\Gamma_{[M]})$ and write $A = A_1 | \dots | A_k$, $B = B_1 | \dots | B_k$. It suffices to show that there exists a (k, k) -partition C such that $I_{AC} = M = I_{CB}$, i.e. that $A - C - B$ is a path of length 2. We will do this by describing an explicit construction for C . Define $I'_{AB} := \frac{1}{k} I_{AB}$. Then I'_{AB} is a doubly stochastic matrix. By Lemma 3.4.20, I'_{AB} and therefore $I_{AB} = k I'_{AB} := (a_{st})$, has a positive diagonal. Moreover, the latter diagonal has positive integer entries, in particular at least 1. Denote this diagonal by $D = (a_{i_1 j_1}, \dots, a_{i_k j_k})$, where for $r \in \{1, \dots, k\}$, $S_{i_r j_r} := A_{i_r} \cap B_{j_r}$ and $a_{i_r j_r} = |S_{i_r j_r}| \geq 1$. Let C_1 be a k -subset which consists of exactly one element from each intersection $S_{i_r j_r}$, for $r \in \{1, \dots, k\}$. Then $|C_1| = k$ and $|A_i \cap C_1| = 1 = |C_1 \cap B_i|$ for all $i \in \{1, \dots, k\}$. Note that if we subtract 1 from each of the entries $a_{i_r j_r}$ in I_{AB} then the matrix $I_{AB}^{(1)}$ which remains is a $(k-1)$ -doubly stochastic matrix where $(I_{AB}^{(1)})_{i_r j_r} = |(A_{i_r} \cap B_{j_r}) \setminus C_1|$ for $r \in \{1, \dots, k\}$, and $(I_{AB}^{(1)})_{st} = (I_{AB})_{st}$ otherwise. As before Lemma 3.4.20 asserts that $I_{AB}^{(1)} := (b_{st})$ has a positive integer diagonal, say $D' = (b_{t_1 u_1}, \dots, b_{t_k u_k})$, where for $r \in \{1, \dots, k\}$, either $b_{t_r u_r} = |(A_{t_r} \cap B_{u_r}) \setminus C_1|$ or $b_{t_r u_r} = |A_{t_r} \cap B_{u_r}|$. In the former case define $T_{t_r u_r} := (A_{t_r} \cap B_{u_r}) \setminus C_1$ and in the latter case define

$T_{t_r u_r} := A_{t_r} \cap B_{u_r}$. Note that in either case $T_{t_r u_r} \cap C_1 = \emptyset$. Now let C_2 be a k -subset which consists of exactly one element from each of the sets $T_{t_r u_r}$, for $r \in \{1, \dots, k\}$. Then $|C_2| = k$, $|A_i \cap C_2| = 1 = |C_2 \cap B_i|$ for all $i \in \{1, \dots, k\}$, and we construct the $(k-2)$ -doubly stochastic matrix $I_{AB}^{(2)}$ in an analogous way to $I_{AB}^{(1)}$. We may repeat the above process to construct a k -subset C_j at which stage we are left with a $(k-j)$ -doubly stochastic matrix. Then we can construct C_{j+1} as long as $k-j \geq 1$, i.e. $j+1 \leq k$. In this way we may construct sets $C_1, \dots, C_k$ such that $|C_j| = k$ and $|A_i \cap C_j| = 1 = |C_j \cap B_i|$ for all $i, j \in \{1, \dots, k\}$. The sets C_j are disjoint by construction. Lastly, define $C := C_1 \dots C_k$. Then $I_{AC} = M = I_{CB}$, and hence $A - C - B$ is a path of length 2. $\square$

3.5 Action of $G := S_n$ and A_n on $(G : H)$, where H is primitive

In this section we prove Theorems 3.2.5(3), 3.2.6(3) and 3.2.8(3).

We will need the following result concerning the orders of primitive subgroups of S_n and A_n .

Lemma 3.5.1 (Corollary 1.2 in [18]). *If H is a primitive subgroup of S_n not containing A_n , then $|H| < 3^n$. Moreover, if $n > 24$, then $|H| < 2^n$.*

In the following, e denotes the base of the natural logarithm.

Proof of Theorem 3.2.5(3). Suppose $\text{diam}_O(G, \Omega) \leq c$. Then (G, Ω) has an orbital graph of diameter $d \leq c$. Hence by Lemma 2.2.1

$$|G : H| \leq 1 + 2|H| + 2|H|(2|H| - 1) + \dots + 2|H|(2|H| - 1)^{c-1} < (2|H|)^{c+1}. \quad (3.19)$$

Using Lemma 3.5.1 and (3.19) we obtain that either $n \leq 24$ or $n!/2 < 2^{(c+1)(n+1)+n}$. Now $n!/2 > (n/e)^n$ (this follows from (8.8) in [10, p. 161]).

If $n > 24$, then using this and the fact that $(n+1)/n \leq \epsilon = 1.04$, we obtain

$$n < e 2^{\epsilon(c+1)+1} < 2^{\epsilon(c+1)+3}. \quad (3.20)$$

Note that (3.20) also holds for $n \leq 24$ (using any $c \geq 1$) and hence holds for all n . $\square$

We now work towards proving Theorem 3.2.6(3).

Proposition 3.5.2. *Let (G, Ω) be a finite primitive permutation group with $G := S_n$ or A_n and $\Omega := (G : H)$, where $H \neq A_n$ is primitive on $\{1, \dots, n\}$. If $\text{diam}_O(G, \Omega) \leq 5$, then n and H are in Tables 3.9 or 3.10, respectively.*

n	H
5	$\text{AGL}_1(5)$
6	$\text{PGL}_2(5)$
7	$\text{AGL}_1(7)$
8	$\text{PGL}_2(7)$
9	$\text{AGL}_2(3)$
10	$\text{PGL}_2(9)$
11	$\text{AGL}_1(11)$
12	$\text{PGL}_2(11)$
14	$\text{PGL}_2(13)$
18	$\text{PGL}_2(17)$

Table 3.9: Possible pairs (n, H) with $\text{diam}_O(S_n, \Omega) \leq 5$, where $\Omega := (S_n : H)$ and H is primitive

n	H
5	D_{10}
6	$\text{PSL}_2(5)$
7	$\text{PSL}_3(2)$
8	$\text{ASL}_3(2)$
9	$\text{ASL}_2(3), \text{PTL}_2(8)$
10	M_{10}
11	M_{11}
12	M_{12}
13	$\text{PSL}_3(3)$
14	$\text{PSL}_2(13)$
15	$\text{PSL}_4(2)$
16	$2^4.\text{PSL}_4(2)$
17	$\text{PTL}_2(16)$
23	M_{23}
24	M_{24}

Table 3.10: Possible pairs (n, H) with $\text{diam}_O(A_n, \Omega) \leq 5$, where $\Omega := (A_n : H)$ and H is primitive

Proof. Suppose $\text{diam}_O(G, \Omega) \leq 5$. Then (G, Ω) has an orbital graph of diameter $d \leq 5$. Using Lemma 3.5.1 and Lemma 2.2.1, we obtain that either $n \leq 24$ or

$$|G| \leq 2^n(1 + 2^{n+1} + 2^{n+1}(2^{n+1} - 1) + 2^{n+1}(2^{n+1} - 1)^2 + 2^{n+1}(2^{n+1} - 1)^3 + 2^{n+1}(2^{n+1} - 1)^4).$$

Using this we can deduce that $n \leq 173$ for $G = S_n$ and $n \leq 174$ for $G = A_n$; let $L_{[n]}$ denote the list consisting of these values. We then use the computer program $C_{\text{VAL}}^G(5, L_{[n]})$ (detailed in Section 5.4 in Chapter 5) to output the values of n for which there exist primitive subgroups H of G satisfying (2.2) from Lemma 2.2.1 with $d = 5$. We find that the output is $5 \leq n \leq 28$, $n \neq 15, 16, 19, 23$ for $G = S_n$, and $5 \leq n \leq 32$, $n \neq 19, 29, 30$ for $G = A_n$. Let $L_{[n_{\text{new}}]}$ denote the new list of values of n outputted. We then use an-

other computer program, namely $C_{\text{LOW}}^G(5, L_{[n_{\text{new}}]})$ (detailed in Section 5.5 in Chapter 5) to output a final list of values of n for which the lower bound for the diameter in Proposition 2.2.2 is strictly less than 5. Thus the permutation groups corresponding to each discarded value of n have orbital graphs of diameter at least 6 and hence these discarded values cannot occur. Each entry in the final list is a pair which consists a value of n together with a primitive subgroup H from the database of primitive permutation groups in (the computational algebra system) Magma. The final values of n and the subgroups H obtained are precisely the ones in Table 3.9 for $G = S_n$ and in Table 3.10 for $G = A_n$. $\square$

Proof of Theorem 3.2.6(3). If $\text{diam}_O(G, X) \leq 5$, then by Proposition 3.5.2, the pair (n, H) must be in Table 3.9 for $G = S_n$ and Table 3.10 for $G = A_n$. Let $L_{[n]}$ denote the list consisting of these values of n . We use the computer program $C_{\text{DIAM}}^G(5, L_{[n]})$ (detailed in Section 5.6 in Chapter 5) to output the diameters of the orbital graphs of (G, X) and verify that the only pairs (n, H) for which $\text{diam}_O(G, X) \leq 5$, are the ones in Table 3.2 for $G = S_n$ and in Table 3.3 for $G = A_n$. This program also outputs the rank of (G, X) , the valencies of the orbital graphs, and identifies the corresponding subgroups H with groups from the database of primitive permutation groups in Magma. Note that $C_G^{\text{DIAM}}(5, [n])$ fails to analyse the cases mentioned in Remark 3.2.7(1) due to limitations of the program which are described in Section 5.1 in Chapter 5. $\square$

Proof of Theorem 3.2.8(3). Suppose (G, X) has an orbital graph of diameter 2. Then using Lemma 3.5.1 and Lemma 2.2.1, we obtain that either $n \leq 24$ or

$$|G| \leq 2^n(1 + 2^{n+1} + 2^{n+1}(2^{n+1} - 1)).$$

One can check that no value of $n > 24$ satisfies the above inequality and hence we have $n \leq 24$ for both $G = S_n$ and $G = A_n$; let $L_{[n]}$ denote the list consisting of these values. We use the computer program $C_{\text{VAL}}^G(2, L_{[n]})$

(detailed in Section 5.4 in Chapter 5) to output the values of n for which there exist primitive subgroups H of G satisfying (2.2) from Lemma 2.2.1 with $d = 2$. Let $L_{[n_{\text{new}}]}$ denote the new list of values of n outputted. We then use the computer program $C_{\text{DIAM}}^G(2, L_{[n_{\text{new}}]})$ (detailed in Section 5.6 in Chapter 5) to output the diameters of the orbital graphs of (G, X) and verify that the only pairs of (n, H) for which (G, X) has an orbital graph of diameter 2, are the ones in Table 3.4 for $G = S_n$ and in Table 3.5 for $G = A_n$. As before, this program also outputs the rank of (G, X) , the valencies of the orbital graphs, and identifies the corresponding subgroups H with groups from the database of primitive permutation groups in Magma. Note that $C_G^{\text{DIAM}}(2, [n])$ fails to analyse the case $n = 24$ for $G = A_n$ due to limitations of the program which are described in Section 5.1 in Chapter 5. $\square$

Chapter 4

The projective special linear groups of dimension 2

In this chapter we study the orbital diameters of the primitive actions of almost simple groups with socle isomorphic to the projective special linear group $\mathrm{PSL}_2(q)$, for q odd. We give necessary conditions for the orbital diameters to be bounded above by 2 and to some extent make the conditions precise. For each primitive action, we also give information about orbital graphs of diameter 2.

The chapter is split into seven sections. In Sections 4.1 and 4.2, we state the preliminary results that are needed for the chapter, and then state the main result of the chapter. We devote Sections 4.3, 4.4, 4.5 and 4.6 to analysing the primitive actions which arise from the different maximal subgroups of $\mathrm{PSL}_2(q)$, and we give a proof of the main result in Section 4.7.

4.1 Preliminary theory

In this section we present the background material which will be needed throughout the chapter.

We begin by stating formulas for orders of the groups $\mathrm{PGL}_2(q)$ and $\mathrm{PSL}_2(q)$; see [[24, p. 44]] for the following result.

Lemma 4.1.1. *We have $|\mathrm{PGL}_2(q)| = q(q^2 - 1)$ and $|\mathrm{PSL}_2(q)| = \frac{q(q^2-1)}{2}$.*

When analysing the primitive actions of $\mathrm{PSL}_2(q)$, we will often treat $\mathrm{PSL}_2(q)$ as an orthogonal group. In particular, we will make use of the following isomorphisms.

Proposition 4.1.2. *We have the following isomorphisms:*

1. $\mathrm{PSL}_2(q) \cong \Omega_3(q)$, for q odd (Proposition 2.9.1(v) in [14]);
2. $\mathrm{PGL}_2(q) \cong \mathrm{SO}_3(q)$ (Theorem 11.6 in [23]);
3. $\mathrm{PSL}_2(q^2) \cong \Omega_4^-(q)$ (Corollary 11.8 in [23]).

In some sections of the chapter, we will need to determine whether or not a given element of $O(V)$ belongs to $\Omega(V)$. To do this we shall use the following theory.

Definition 4.1.3. Let (V, Q) be a quadratic space and let $v \in V$ with $Q(v) \neq 0$. We define the *reflection* in v as the map $r_v : V \rightarrow V$ given by $x \mapsto x - \frac{(v, x)}{Q(v)}v$.

Proposition 4.1.4 ([14, p. 29]). *Let (V, Q) be a non-degenerate quadratic space over $\mathbb{F}_q$ where q is odd. Then $O(V) = \langle r_v : Q(v) \neq 0 \rangle$. Moreover, $\mathrm{SO}(V)$ consists of the elements of $O(V)$ that can be written as a product of an even number of reflections.*

Definition 4.1.5. Let (V, Q) be a non-degenerate quadratic space over $\mathbb{F}_q$ where q is odd and let $g := r_{v_1} \cdots r_{v_k} \in \mathrm{SO}(V)$ be a product of reflections. The *spinor norm* of g is defined to be 1 if the product $\prod_{i=1}^k (v_i, v_i)$ is a square in $\mathbb{F}_q$, and -1 otherwise.

For the next result, see Proposition 2.5.7 and Description 1 in [14, p. 29].

Proposition 4.1.6. *Let (V, Q) be a non-degenerate quadratic space over $\mathbb{F}_q$ where q is odd. Then $\Omega(V)$ consists of all the elements of $\mathrm{SO}(V)$ whose spinor norm is 1, and is the unique subgroup of $\mathrm{SO}(V)$ of index 2.*

We now state an important result which will be used many times in the chapter.

Lemma 4.1.7 (Witt's Lemma). *([1, p. 81]). Let (V, κ) be a symplectic, unitary or quadratic space. Let U and W be subspaces of V and suppose $g : U \rightarrow V$ is an isometry. Then g extends to an isometry of V .*

In the chapter we will not only be analysing the simple groups $\mathrm{PSL}_2(q)$, but more generally we will be analysing almost simple groups with socle isomorphic to $\mathrm{PSL}_2(q)$, i.e. groups G satisfying $\mathrm{PSL}_2(q) \leq G \leq \mathrm{Aut}(\mathrm{PSL}_2(q))$. For a group G and $\dot{\Gamma} \leq \mathrm{Aut}(G)$, we will denote by $\ddot{\Gamma}$, the image of $\dot{\Gamma}$ in $\mathrm{Out}(G)$, and similarly for $\dot{f} \in \mathrm{Aut}(G)$.

Remark 4.1.8. Let G be an almost simple group with socle S . If H is a maximal subgroup of G and H contains S , then S acts trivially on $(G : H)$. For the purposes of the thesis, we are not interested in these kinds of actions, and therefore when looking at primitive actions of almost simple groups, we will exclude the cases where the socle is contained in the maximal subgroup.

To analyse the primitive actions of almost simple groups with socle isomorphic to $\mathrm{PSL}_2(q)$, we will require explicit knowledge of automorphisms of $\mathrm{PSL}_2(q)$.

Definition 4.1.9. Let q be a power of the odd prime p .

1. Define $\dot{\delta}$ to be the automorphism of $\mathrm{PSL}_2(q)$ which maps the coset containing $A \in \mathrm{SL}_2(q)$ to the coset containing the matrix $D^{-1}AD$, where D is a diagonal matrix with diagonal entries μ and 1, and μ is a generator of $\mathbb{F}_q^*$.

2. Define $\dot{\phi}$ to be the automorphism of $\mathrm{PSL}_2(q)$ which maps the coset containing $A \in \mathrm{SL}_2(q)$ to the coset containing the matrix A with each entry replaced by its p^{th} power.

The next result follows from Propositions 2.2.2 and 2.2.3 in [14].

Proposition 4.1.10. *Let $\dot{\delta}$ and $\dot{\phi}$ be as above. Then the following hold:*

1. $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \langle \mathrm{PSL}_2(q), \dot{\delta}, \dot{\phi} \rangle;$
2. $\mathrm{Out}(\mathrm{PSL}_2(q)) = \langle \ddot{\delta}, \ddot{\phi} \rangle;$
3. $\langle \mathrm{PSL}_2(q), \dot{\delta} \rangle \cong \mathrm{PGL}_2(q).$

We will also need a description of the conjugacy classes of maximal subgroups of G , where $\mathrm{soc}(G) \cong \mathrm{PSL}_2(q)$. The following result can be found in a more general context as Theorem 2.1.1 in [3]. Recall that D_n denotes a dihedral group of order n .

Theorem 4.1.11. *Let $q \geq 5$ be a power of the odd prime p and let G be an almost simple group with $S := \mathrm{soc}(G) \cong \mathrm{PSL}_2(q)$. Then representatives of the conjugacy classes of maximal subgroups H of G that do not contain S can be read off from Table 4.1.*

$H \cap S$	Notes	c	Stab
P_1		1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
D_{q-1}	$q \neq 5, 7, 9, 11$	1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
	$q = 7, 11$ N1	1	$\langle \ddot{\delta} \rangle$
	$q = 9$ N2	1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
D_{q+1}	$q \neq 7, 9$	1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
	$q = 7$ N1	1	$\langle \ddot{\delta} \rangle$
	$q = 9$ N2	1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
$\text{PGL}_2(q_0)$	$q = q_0^2$	2	$\langle \ddot{\phi} \rangle$
$\text{PSL}_2(q_0)$	$q = q_0^t, t$ odd prime	1	$\langle \ddot{\delta}, \ddot{\phi} \rangle$
S_4	$q = p \equiv \pm 1 \pmod{8}$	2	1
A_4	$q = p \equiv \pm 3, 5, \pm 13 \pmod{40}$	1	$\langle \ddot{\delta} \rangle$
	$q = p \equiv \pm 11, \pm 19 \pmod{40}$ N1	1	$\langle \ddot{\delta} \rangle$
A_5	$q = p \equiv \pm 1 \pmod{10}$	2	1
	$q = p^2, p \equiv \pm 3 \pmod{10}$	2	$\langle \ddot{\phi} \rangle$

Table 4.1: Maximal subgroups of G , where $\text{soc}(G) \cong \text{PSL}_2(q)$ and q is odd

Explanation of columns in Table 4.1:

- **‘ $H \cap S$ ’:** This column describes the structure of $H \cap S$.
- **‘Notes’:** This column describes restrictions on the values of q .
- **‘ c ’:** This column specifies the number of conjugacy classes in S of subgroups isomorphic to $H \cap S$.
- **‘Stab’:** For a maximal subgroup K of S , the natural action of $\text{Aut}(S)$ on the set of conjugacy classes of subgroups isomorphic to K , is transitive with kernel $\text{Inn}(S)$. Thus it induces a transitive action of $\text{Out}(S)$. This column specifies the stabiliser of one conjugacy class under the latter action. If the ‘Notes’ column of this entry is not marked with ‘N1’ or ‘N2’, then let $\ddot{\Gamma}$ be the subgroup of $\text{Out}(S)$ specified by the

column. For any subgroup T of $\ddot{\Gamma}$, the subgroup $K.T$ is a maximal subgroup of $S.T$. If the entry in this column is ‘N1’, then this is true only when $T = \langle \ddot{\delta} \rangle$. If the entry in this column is ‘N2’, then this is true only when T is not contained in $\langle \ddot{\phi} \rangle$.

Remark 4.1.12. The group $H := P_1$ in Table 4.1 is a *parabolic* subgroup of $G := \text{PSL}_2(q)$ and the action of G on $(G : H)$ is equivalent to the natural action of G on 1-dimensional subspaces of the vector space $\mathbb{F}_q^2$ (see Proposition 6.3.1 in Chapter 6), which can easily be seen to be 2-transitive.

4.2 Statement of the main result

We now state the main result of the chapter.

Theorem 4.2.1. *Let $q \geq 17$ be odd and let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $S \not\leq H <_{\max} G$.*

1. *If $\text{diam}_O(G, X) \leq 2$, then $H \cap S$ is isomorphic to one of the following:*

- P_1 ;
- $\text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 3 \pmod{4}$;
- $\text{PSL}_2(q^{1/3})$.

Furthermore, the converse is known in all cases apart from $\text{PSL}_2(q^{1/3})$.

2. *Suppose $G \cong \text{PSL}_2(q)$.*

- (a) *If $H \cong D_{q-1}$ with $q \equiv 3 \pmod{4}$, or $H \cong \text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 3 \pmod{4}$, then (G, X) has an orbital graph of diameter 2.*
- (b) *If $H \cong D_{q+1}$, or $H \cong \text{PSL}_2(q^{1/t})$ with t an odd prime, then (G, X) has no orbital graph of diameter 2.*
- (c) *If $H \cong A_4, S_4$ or A_5 , then (G, X) has an orbital graph of diameter 2 if and only if the value of q is as in Table 4.9 (which can be found in Section 4.6).*

Remark 4.2.2.

1. If G and H are as in the statement of Theorem 4.2.1 and $G \cong \text{PSL}_2(q)$, then the existence of orbital graphs of diameter 2 is undetermined for the cases $H \cong D_{q-1}$ with $q \equiv 1 \pmod{4}$, and $\text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 1 \pmod{4}$. See Conjecture 4.4.2 for the latter case.
2. The orbital diameters of primitive actions of almost simple groups G with $\text{soc}(G) \cong \text{PSL}_2(q)$ when $q \leq 13$ is odd, can be read off from Table 4.2 (see the end of Section 4.7 for information on how the results in Table 4.2 have been obtained). The cases $H \cap S = P_1$ have been excluded from Table 4.2 as (G, X) is known to be 2-transitive in these cases.
3. We have obtained partial results on primitive actions of almost simple groups G with $\text{soc}(G) \cong \text{PSL}_2(q)$, where q is even, but these have not been included in the thesis.

q	G/S	$H \cap S$	Diameters of orbital graphs	Valencies of orbital graphs
5	1	D_6	2, 2	3, 6
5	$\langle \ddot{\delta} \rangle$	D_6	2, 2	3, 6
5	1	A_4	1	4
5	$\langle \ddot{\delta} \rangle$	A_4	1	4
7	$\langle \ddot{\delta} \rangle$	D_6	4, 3, 3, 2	3, 6, 6, 12
7	$\langle \ddot{\delta} \rangle$	D_8	3, 2, 2	4, 8, 8
7	1	S_4	1	6
9	$\langle \ddot{\delta} \rangle$	D_8	4, 3, 3, 2, 2	4, 8, 8, 8, 16
9	$\langle \ddot{\delta} \ddot{\phi} \rangle$	D_8	4, 2, 2, 2	4, 8, 16, 16
9	$\langle \ddot{\delta}, \ddot{\phi} \rangle$	D_8	4, 2, 2, 2	4, 8, 16, 16
9	$\langle \ddot{\delta} \rangle$	D_{10}	3, 2, 2, 2	5, 10, 10, 10
9	$\langle \ddot{\delta} \ddot{\phi} \rangle$	D_{10}	3, 2, 2	5, 10, 20
9	$\langle \ddot{\delta}, \ddot{\phi} \rangle$	D_{10}	3, 2, 2	5, 10, 20
9	1	$\text{PGL}_2(3)$	2, 2	6, 8
9	$\langle \ddot{\phi} \rangle$	$\text{PGL}_2(3)$	2, 2	6, 8
9	1	A_5	1	5
9	$\langle \ddot{\phi} \rangle$	A_5	1	5
11	$\langle \ddot{\delta} \rangle$	D_{10}	4, 3, 3, 3, 3, 2	5, 10, 10, 10, 10, 20
11	1	D_{12}	3, 3, 3, 3, 2, 2	6, 6, 6, 12, 12, 12
11	$\langle \ddot{\delta} \rangle$	D_{12}	3, 3, 3, 2, 2	6, 12, 12, 12, 12
11	$\langle \ddot{\delta} \rangle$	A_4	4, 3, 3, 2, 2	4, 6, 8, 12, 24
11	1	A_5	1	10
13	1	D_{12}	4, 4, 4, 3, 3, 3, 3, 3	6, 6, 6, 12, 12, 12, 12, 12, 12
13	$\langle \ddot{\delta} \rangle$	D_{12}	4, 3, 3, 3, 3, 3, 2	6, 12, 12, 12, 12, 12, 24
13	1	D_{14}	3, 3, 3, 3, 3, 3, 2	14, 14, 14, 7, 7, 7, 14
13	$\langle \ddot{\delta} \rangle$	D_{14}	3, 3, 3, 3, 3, 2	7, 14, 14, 14, 14, 14
13	1	A_4	5, 5, 5, 4, 3, 3, 3, 3, 2	4, 4, 4, 6, 12, 12, 12, 12, 24
13	$\langle \ddot{\delta} \rangle$	A_4	5, 4, 3, 3, 3, 2, 2	4, 6, 8, 12, 12, 24, 24

Table 4.2: Diameters of orbital graphs of (G, X) , where $\text{soc}(G) \cong \text{PSL}_2(q)$ and $q \leq 13$ is odd

4.3 $H \cap S \cong D_{q\pm 1}$

In this section we analyse the diameters of the orbital graphs of the action of G on cosets of maximal subgroups H , where $S := \text{soc}(G) \cong \text{PSL}_2(q)$ (q odd) and $H \cap S \cong D_{q\pm 1}$. We first state the two main theorems that we will prove in this section.

Theorem 4.3.1. *Let $q \geq 13$ be odd and let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong D_{q-1}$.*

1. *There exist no values of q such that $\text{diam}_O(G, X) \leq 2$.*
2. *If $q \equiv 3 \pmod{4}$, then (G, X) has an orbital graph of diameter 2.*

Moreover, if $G \cong \text{PGL}_2(q)$ then $\text{diam}_O(G, X) \leq 3$ for all $q \geq 17$, and (G, X) has an orbital graph of diameter 2 for all q .

Theorem 4.3.2. *Let $q \geq 11$ be odd and let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong D_{q+1}$.*

1. *There exist no values of q such that $\text{diam}_O(G, X) \leq 2$.*
2. *If $q \geq 17$ and $G \cong \text{PSL}_2(q)$ or $\text{PGL}_2(q)$, then (G, X) has no orbital graphs of diameter 2.*

Let (G, X) be as in Theorem 4.3.2. Although there are no orbital graphs of diameter 2 when $G \cong \text{PSL}_2(q)$ or $\text{PGL}_2(q)$, computations suggest that orbital graphs of diameter 2 do occur for other groups G . In particular, we conjecture the following result which has been verified for values of $q \leq 243$ using a computer.

Conjecture 4.3.3. *Let $q \geq 11$ be odd and suppose q is not a prime. Let (G, X) be a primitive permutation group with $G := \text{Aut}(\text{PSL}_2(q))$ and $X := (G : H)$, where $H \cap \text{PSL}_2(q) \cong D_{q+1}$. Then (G, X) has an orbital graph of diameter 2.*

In order to prove Theorems 4.3.1 and 4.3.2, we will consider $\mathrm{PSL}_2(q)$ as a subgroup of the 3-dimensional orthogonal group $O_3(q)$. Let q be odd and let V be a 3-dimensional vector space over $\mathbb{F}_q$ equipped with a non-degenerate quadratic form. Recall that the group $O(V) \cong O_3(q)$ stabilises the quadratic form. Also recall that $\mathrm{SO}(V) = O(V) \cap \mathrm{SL}(V) \cong \mathrm{SO}_3(q)$ and $\Omega(V) \cong \Omega_3(q)$ is the unique subgroup of $\mathrm{SO}(V)$ of index 2. Now by Proposition 4.1.2, we have $\mathrm{PSL}_2(q) \cong \Omega_3(q)$. We shall see later that under this isomorphism the maximal subgroups of $\mathrm{PSL}_2(q)$ which are dihedral, are stabilisers of certain 1-dimensional subspaces of V .

We now describe the automorphism group of $\Omega_3(q)$. Recall that by Proposition 2.3.11, the underlying vector space has a standard basis $\{e_1, f_1, x\}$; henceforth, for simplicity we will write $e := e_1$ and $f := f_1$, and we will assume $Q(x) = 1/2$, i.e. $(x, x) = 1$ (see Remark 4.3.4).

Remark 4.3.4. By Proposition 2.5.4(ii) in [14], the two isometry classes of non-degenerate quadratic spaces of odd dimensions are distinguished by whether or not $Q(x)$ is a square. As all the quadratic spaces of dimension n are similar, for the purposes of analysing primitive actions, we may suppose $Q(x)$ is a square or non-square as convenient (see Remark 2.3.8). Moreover, by replacing x by a suitable scalar multiple of itself, we may assume that $Q(x)$ is any non-zero element of $\mathbb{F}_q$ which is convenient.

Definition 4.3.5. Let V be as above where q is a power of the odd prime p , and let $\{e, f, x\}$ be the standard basis. We define ϕ to be the map $V \rightarrow V$, given by $ae + bf + cx \mapsto a^p e + b^p f + c^p x$, for $a, b, c \in \mathbb{F}_q$, and we define $\dot{\phi}$ to be the map $O_3(q) \rightarrow O_3(q)$ given by $g \mapsto \phi^{-1} g \phi$. Fix a non-square $\gamma \in \mathbb{F}_q$. We define $\delta := r_x r_{e + \frac{\gamma}{2} f}$, and $\dot{\delta}$ is defined analogously to $\dot{\phi}$.

Remark 4.3.6. Let $\{e, f, x\}$ be the standard basis. For $u, v \in V$ write $u = a_1 e + b_1 f + c_1 x$ and $v = a_2 e + b_2 f + c_2 x$, where $a_i, b_i, c_i \in \mathbb{F}_q$. Then

$$(u^\phi, v^\phi) = (a_1 b_2)^p + (a_2 b_1)^p + (c_1 c_2)^p = ((a_1 b_2) + (a_2 b_1) + (c_1 c_2))^p = (u, v)^p.$$

Using this, it is straightforward to see that if $g \in O_3(q)$, then $\phi^{-1}g\phi$ and $\delta^{-1}g\delta$ preserve the form, and thus $\dot{\phi}(g), \dot{\delta}(g) \in O_3(q)$. One can also easily check that $\dot{\phi}$ and $\dot{\delta}$ are bijective homomorphisms, i.e. automorphisms of $O_3(q)$.

Lemma 4.3.7. *The maps $\dot{\delta}$ and $\dot{\phi}$ are automorphisms of $\Omega_3(q)$.*

Proof. By Remark 4.3.6, it suffices to show that $\dot{\phi}(\Omega_3(q)) = \Omega_3(q)$, and the same with $\dot{\delta}$. Now, it is straightforward to check that if $\det(g) = 1$, then $\det(\phi^{-1}g\phi) = 1$ and the same with δ , and thus $\dot{\phi}$ and $\dot{\delta}$ are automorphisms of $\text{SO}_3(q)$. Further, it is an easily proved fact that the commutator subgroup H of a group G satisfies $f(H) \leq H$ for all $f \in \text{Aut}(G)$. Since $\Omega_3(q)$ is the commutator subgroup of $\text{SO}_3(q)$, this implies that $\dot{\phi}(\Omega_3(q)) \leq \Omega_3(q)$ and the equality follows since we also have $\dot{\phi}^{-1}(\Omega_3(q)) \leq \Omega_3(q)$. $\square$

Proposition 4.3.8. *Let $\dot{\delta}$ and $\dot{\phi}$ be as above. Then the following hold:*

1. $\text{Aut}(\Omega_3(q)) = \langle \text{Inn}(\Omega_3(q)), \dot{\delta}, \dot{\phi} \rangle$;
2. $\langle \text{Inn}(\Omega_3(q)), \dot{\delta} \rangle \cong \text{SO}_3(q)$.

Proof. By Lemma 4.3.7, we have $A := \langle \text{Inn}(\Omega_3(q)), \dot{\delta}, \dot{\phi} \rangle \leq \text{Aut}(\Omega_3(q))$. Now δ has spinor norm -1 and $\delta^2 = 1$, thus $\ddot{\delta}$ has order 2. Let $q = p^r$, where p is an odd prime. The map $\dot{\phi}$ maps a matrix $M := (m_{ij})$ to the matrix $M^p := (m_{ij}^p)$, and therefore $\dot{\phi}^r = 1$. Moreover, no power of $\dot{\phi}$ strictly less than r is an inner automorphism of $\Omega_3(q)$ and thus $\ddot{\phi}$ has order r . Recall that $\ddot{\delta}$ and $\ddot{\phi}$ denote the images of $\dot{\delta}$ and $\dot{\phi}$ in $\text{Out}(\Omega_3(q))$, respectively. Now one can check that $\ddot{\phi}\ddot{\delta} = \ddot{\delta}\ddot{\phi}$ and hence $A/\text{Inn}(\Omega_3(q)) = \langle \ddot{\delta}, \ddot{\phi} \rangle \cong C_2 \times C_r$. Thus $|A| = 2r|\text{Inn}(\Omega_3(q))| = |\text{Aut}(\Omega_3(q))|$, where the final equality follows from Proposition 2.6.3 in [14]. Hence $A = \text{Aut}(\Omega_3(q))$ which proves part 1. Part 2 follows by observing that $\langle \text{Inn}(\Omega_3(q)), \dot{\delta} \rangle \cong \langle \Omega_3(q), \delta \rangle \leq \text{SO}_3(q)$, and then comparing orders. $\square$

Remark 4.3.9. The information on maximal subgroups of almost simple groups with socle $\text{PSL}_2(q)$ in Table 4.1, can be translated to information

on maximal subgroups of almost simple groups with socle $\Omega_3(q)$ with δ and ϕ as in Definition 4.3.5 (see Table 8.7 in [3] for maximal subgroups of the latter).

Let X denote the set of all 1-dimensional subspaces of V . For the remainder of this section, we shall use X_s and X_n to denote the set of elements $\langle v \rangle \in X$ with (v, v) a square and a non-square, respectively. Note that if $\langle v \rangle$ is in X_s or X_n , then without loss of generality we may assume that $(v, v) = 1$ or $(v, v) = \gamma$ (where γ is the non-square in Definition 4.3.5), respectively.

Lemma 4.3.10. *We have $|X_s| = \frac{q(q+1)}{2}$ and $|X_n| = \frac{q(q-1)}{2}$.*

Proof. The size of X_s is the number of 1-dimensional subspaces $\langle v \rangle$ with (v, v) a square; we may suppose that this square is 1. Note that $(-v, -v) = (v, v)$ and thus $|X_s|$ is half the number of vectors v such that $(v, v) = 1$. Let $\{e, f, x\}$ be the standard basis and write $v = ae + bf + cx$, where $a, b, c \in \mathbb{F}_q$. Then $(v, v) = 2ab + c^2$. If $b = 0$, then there are $2q$ solutions to $(v, v) = 1$, which are $(a, b, c) = (a, 0, \pm 1)$. If $b \neq 0$, then there are $q(q-1)$ solutions to $(v, v) = 1$, which are $(a, b, c) = (\frac{1-c^2}{2b}, b, c)$. Hence, the number of vectors v such that $(v, v) = 1$, is $q(q-1) + 2q = q(q+1)$. The result for X_s follows. Similarly, the size of X_n is the number of 1-dimensional subspaces $\langle v \rangle$ with (v, v) a non-square and we may suppose that this non-square is γ . Then $|X_n|$ is half the number of vectors v such that $(v, v) = \gamma$ and as above one can show that the number of such vectors is $q(q-1)$ (the case $b = 0$ doesn't occur). This completes the proof. $\square$

Let G be an almost simple group with $\text{soc}(G) \cong \Omega_3(q)$. Then by Proposition 4.3.8, we have $G = \langle \Omega_3(q), \dot{\Gamma} \rangle$, where $\dot{\Gamma} \leq \langle \dot{\delta}, \dot{\phi} \rangle$. We would like to define an action of G on the sets X_s and X_n ; the groups $\text{SO}_3(q)$ and hence $\Omega_3(q)$ act naturally on these sets, and for $v \in V$ we define $\langle v \rangle^{\dot{\delta}} := \langle v^{\delta} \rangle$ and $\langle v \rangle^{\dot{\phi}} := \langle v^{\phi} \rangle$ (one can easily check that if $\langle v \rangle$ is in X_s (resp. X_n), then $\langle v^{\delta} \rangle$ and $\langle v^{\phi} \rangle$ are both in X_s (resp. X_n)).

Proposition 4.3.11. *The natural actions of $G := \mathrm{SO}_3(q)$ on X_s and X_n are transitive. Moreover, for $\alpha \in X_s$ and $\beta \in X_n$, we have $G_\alpha \cong O_2^+(q) \cong D_{2(q-1)}$ and $G_\beta \cong O_2^-(q) \cong D_{2(q+1)}$.*

Proof. We first prove the statement concerning transitivity. Fix $l \in \{s, n\}$ and let $\alpha, \beta \in X_l$. Write $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$. We may choose v and w such that $(v, v) = (w, w)$ and so the map $i : \alpha \rightarrow \beta$ which maps $\lambda v \mapsto \lambda w$ is an isometry. Hence by Witt's Lemma (Lemma 4.1.7) there exists $g \in O_3(q)$ such that $v^g = w$. Now since every element of $O_3(q)$ has determinant ± 1 ($O_3(q)$ is generated by reflections by Proposition 4.1.4, and each reflection has determinant -1), we have that either $g \in G$ or $-g \in G$. It remains to note that $\alpha^{\pm g} = \beta$.

Note that the isomorphisms $O_2^\pm(q) \cong D_{2(q \mp 1)}$ can be found as Proposition 2.9.1(iii) in [14]. Now let $\{e, f, x\}$ be the standard basis. We have $\langle x \rangle \in X_s$. Since G is transitive on X_s , we have that G_α is conjugate to $G_{\langle x \rangle}$ for all $\alpha \in X_s$. Therefore to prove the first isomorphism in the statement of the result, it suffices to show that $G_{\langle x \rangle} = O_2^+(q)$. Since $\langle x \rangle$ is non-degenerate, we have $V = \langle x \rangle \perp \langle x \rangle^\perp$ (see Remark 2.3.4), and thus $G_{\langle x \rangle} = G_{\langle x \rangle^\perp}$. Now $\langle x \rangle^\perp = \langle e, f \rangle$ contains a 1-dimensional totally singular subspace ($\langle e \rangle$, for example) and thus $G_{\langle x \rangle} = G_{\langle x \rangle^\perp} \leq O_2^+(q)$ (see Proposition 2.5.4(i) in [14]). Now the Orbit-Stabiliser property implies $|G_{\langle x \rangle}| = |G|/|X_s| = \frac{2q(q^2-1)}{q(q+1)} = |O_2^+(q)|$, where we have used Lemma 4.1.1 and Lemma 4.3.10 for the orders of G and X_s . Thus $G_{\langle x \rangle} = O_2^+(q)$. To show the statement $G_\beta \cong O_2^-(q)$, it suffices to show that $G_{\langle e + \frac{\gamma}{2}f \rangle} = O_2^-(q)$. As above $G_{\langle e + \frac{\gamma}{2}f \rangle} = G_{\langle e + \frac{\gamma}{2}f \rangle^\perp} \leq O_2^-(q)$ as $\langle e + \frac{\gamma}{2}f \rangle^\perp = \langle e - \frac{\gamma}{2}f, x \rangle$ contains no 1-dimensional totally singular subspace (see Proposition 2.5.4(i) in [14]), and then the equality follows by comparing orders. $\square$

Corollary 4.3.12. *The natural actions of $S := \Omega_3(q)$ on X_s and X_n are transitive. Moreover, for $\alpha \in X_s$ and $\beta \in X_n$, we have $S_\alpha \cong D_{q-1}$ and $S_\beta \cong D_{q+1}$.*

Proof. We will show that S acts transitively on X_s . The corresponding claim for X_n can be proved similarly and is left to the reader. By (2.5.12) in [14], we have

$$G = S\langle r_x r_y \rangle, \quad (4.1)$$

where $G := \mathrm{SO}_3(q)$, and r_x and r_y are reflections in $x, y \in V$ with (x, x) a square and (y, y) a non-square. Let $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$ be two elements in X_s . By Proposition 4.3.11, G acts transitively on X_s so there exists $g \in G$ such that $\alpha^g = \beta$. Pick $x, y \in \alpha^\perp$ with (x, x) a square and (y, y) a non-square (see the Remark in [14, p. 27] for why this is possible). By (4.1), either $h := g \in S$ or there exists $h \in S$ such that $g = hr_x r_y$. In the latter case, we have $\alpha^{r_x r_y} = \alpha$ and thus in both cases, we have $\alpha^h = \beta$ and $h \in S$. This proves the transitivity of S .

To prove the first isomorphism in the statement of the result, observe that since G and S are transitive on X_s , using the Orbit-Stabiliser property we have $|S_\alpha| = q - 1$. Now S_α must be contained in a maximal subgroup of S , the only possibility for which is D_{q-1} by Table 4.1. Thus by comparing orders we have $S_\alpha \cong D_{q-1}$. A similar argument shows that $S_\beta \cong D_{q+1}$. $\square$

Corollary 4.3.13. *Let $G := \langle S, \dot{\Gamma} \rangle$ be an almost simple group where $S := \mathrm{soc}(G) \cong \Omega_3(q)$ and $\dot{\Gamma} \leq \langle \dot{\delta}, \dot{\phi} \rangle$. Then for $\alpha \in X_s$ and $\beta \in X_n$, we have $G_\alpha = S_\alpha \ddot{\Gamma}$ and $G_\beta = S_\beta \ddot{\Gamma}$, and both point stabilisers are maximal subgroups of G provided $q \geq 13$ and $q \geq 11$, for α and β respectively.*

Proof. We prove the result for α ; the proof for β is similar. By Corollary 4.3.12 and Theorem 4.1.11, S_α is a maximal subgroup of S and thus G_α is a maximal subgroups of G . Now S acts transitively on X_s by Corollary 4.3.12, and thus so does G . This implies $G = G_\alpha S$ and thus

$$\ddot{\Gamma} = \frac{G}{S} = \frac{G_\alpha S}{S} \cong \frac{G_\alpha}{G_\alpha \cap S} = \frac{G_\alpha}{S_\alpha}.$$

$\square$

By Corollary 4.3.13, in order to analyse the primitive actions of G with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ on the cosets of H where $H \cap S \cong D_{q\pm 1}$, it suffices to assume $\text{soc}(G) = \Omega_3(q)$ and analyse the natural actions of G on X_s and X_n . To analyse the latter actions, we will begin by analysing the particular case where $G = \text{SO}_3(q)$. We begin by determining the orbitals of this action.

Proposition 4.3.14. *Let $G := \text{SO}_3(q)$ and $l \in \{s, n\}$. For $l = s$ and $l = n$, define $\alpha := 1$ and $\alpha := \gamma$, respectively. The non-diagonal orbitals of (G, X_l) are*

$$\Delta_{\pm\lambda}^l := \{(\langle v \rangle, \langle w \rangle) \in X_l \times X_l : (v, v) = (w, w) = \alpha, (v, w) = \pm\lambda\alpha\},$$

where $\lambda \in \mathbb{F}_q$ for $l = s$, and $\lambda \in \mathbb{F}_q \setminus \{\pm 1\}$ for $l = n$.

Proof. Let $\{e, f, x\}$ be the standard basis. We firstly verify that the sets $\Delta_{\pm\lambda}^l$ are non-empty for the values of λ in the statement of the result. For $l = s$, let $v := x$ and $w := (1-\lambda)e + (1+\lambda)f + \lambda x$. Then $(\langle v \rangle, \langle w \rangle) \in \Delta_{\pm\lambda}^s$. Now suppose $l = n$. Let $v := e + \frac{\gamma}{2}f$. Since $\langle v \rangle$ is non-degenerate, we have $V = \langle v \rangle^\perp$. Note that $\langle v \rangle^\perp = \langle e - \frac{\gamma}{2}f, x \rangle$. Let $w := a(e + \frac{\gamma}{2}f) + b(e - \frac{\gamma}{2}f) + cx$, for some $a, b, c \in \mathbb{F}_q$. Now $(\langle v \rangle, \langle w \rangle) \in \Delta_{\pm\lambda}^n$ if and only if $(w, w) = \gamma$ and $(v, w) = \pm\lambda\gamma$. These conditions imply the equality $c^2 = \gamma(b^2 - \lambda^2 + 1)$. One can see that the latter equation has no non-zero solutions (b, c) if $\lambda = \pm 1$ and thus since G is transitive on X_n , we conclude that $\Delta_{\pm 1}^n$ is empty. Suppose $\lambda \neq \pm 1$. To show that $\Delta_{\pm\lambda}^n$ is non-empty, it suffices to show that there exists b such that $b^2 - \lambda^2 + 1$ is a non-square. This is equivalent to proving the existence of b, d with $d \neq 0$ such that $b^2 - d^2\gamma = \lambda^2 - 1 \neq 0$. Indeed such b, d exist (see Lemma A.11 in Appendix A). Thus $\Delta_{\pm\lambda}^l$ is non-empty for the values of λ in the statement of the result.

Now fix l . It is straightforward to check that the sets $\Delta_{\pm\lambda}^l$ are disjoint and that their union (together with the diagonal orbital) is $X_l \times X_l$. It is also clear that if $(\langle v_1 \rangle, \langle w_1 \rangle)$ and $(\langle v_2 \rangle, \langle w_2 \rangle)$ are in the same orbital (with $(v_1, v_1) = (v_2, v_2)$ and $(w_1, w_1) = (w_2, w_2)$) then $(v_1, w_1) = \pm(v_2, w_2)$.

It remains to show that G is transitive on $\Delta_{\pm\lambda}^l$. Let $\alpha := (\langle v \rangle, \langle w \rangle)$ and $\beta := (\langle v' \rangle, \langle w' \rangle)$ be two elements of $\Delta_{\pm\lambda}^l$. Let v'' be the vector $\pm v'$ so that $\langle v' \rangle = \langle v'' \rangle$ and $(v, w) = (v'', w')$. Define the map $i : \langle v, w \rangle \rightarrow \langle v', w' \rangle$ which maps $v \mapsto v''$, $w \mapsto w'$ and extends linearly. Then i is an isometry and hence by Witt's Lemma there exists $g \in O_3(q)$ such that $v^g = v''$ and $w^g = w'$. Now since every element of $O_3(q)$ has determinant ± 1 , we have that either $g \in G$ or $-g \in G$. It remains to note that $\alpha^{\pm g} = \beta$. $\square$

We will denote by $\Gamma_{\pm\lambda}^l$ the orbital graph corresponding to the orbital $\Delta_{\pm\lambda}^l$ from Proposition 4.3.14. Note that since the form $(\cdot, \cdot)$ is symmetric, the orbitals $\Delta_{\pm\lambda}^l$ are self-paired and thus the graph $\Gamma_{\pm\lambda}^l$ has vertex set equal to X_l and edges $\{\langle v \rangle, \langle w \rangle\}$, where $(v, v) = (w, w) = \alpha$ and $(v, w) = \pm\lambda\alpha$. We now prove various results concerning the diameters of the graphs $\Gamma_{\pm\lambda}^l$ when $l = s$. Note that if $q \geq 13$ and $\alpha \in X_s$, then S_α is a maximal subgroup of S where $S := \Omega_3(q)$ (see Table 4.1), and so the condition $q \geq 13$ in the results below ensures that the graphs in question are connected.

Proposition 4.3.15. *Let $q \geq 13$. Then $\text{diam}(\Gamma_{\pm 1}^s) = 2$.*

Proof. Let $\{e, f, x\}$ be the standard basis and let $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$ be two distinct elements of X_s . If $(v, w) = \pm 1$, then $d(\alpha, \beta) = 1$. Suppose $(v, w) = \mu$, where $\mu \in \mathbb{F}_q \setminus \{\pm 1\}$. By Remark 2.1.2(2), without loss of generality, we may assume that $v = \frac{1}{2}e + f$ and $w = 2\mu f + x$. Define $u := 2f + x$. Then $(u, u) = 1$ and $(v, u) = (u, w) = 1$. Thus $\langle u \rangle$ is a common neighbour of α and β and so $d(\alpha, \beta) = 2$. The result follows. $\square$

Proposition 4.3.16. *Let $q \geq 13$. Then $\text{diam}(\Gamma_0^s) \geq 3$.*

Proof. Let $\{e, f, x\}$ be the standard basis. Define $v := x$ and $w := f + x$, and $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$. Then $(v, v) = (w, w) = 1$ and so $\alpha, \beta \in X_s$. Now $(v, w) = 1 \neq 0$ and hence $d(\alpha, \beta) \geq 2$. Suppose $d(\alpha, \beta) = 2$ and let $\langle u \rangle$ be a common neighbour of α and β . Write $u = ae + bf + cx$, where $a, b, c \in \mathbb{F}_q$. Then $(u, u) = 1$ implies $2ab + c^2 = 1$, but $(v, u) = (u, w) = 0$

imply $a = c = 0$, which results in a contradiction. Hence $d(\alpha, \beta) \geq 3$ and consequently $\text{diam}(\Gamma_0^s) \geq 3$. $\square$

Proposition 4.3.17. *Let $q \geq 13$. For all $\lambda \in \mathbb{F}_q^*$, we have $\text{diam}(\Gamma_{\pm\lambda}^s) \leq 3$.*

Proof. Let $\{e, f, x\}$ be the standard basis and let $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$ be two distinct elements of X_s . If $(v, w) = \pm\lambda$, then $d(\alpha, \beta) = 1$. Suppose $(v, w) = \mu$, where $\mu \in \mathbb{F}_q \setminus \{\pm\lambda\}$. Without loss of generality, we may assume that $v = \frac{1}{2}\lambda e + \lambda^{-1}f$ and $w = 2\lambda^{-1}\mu f + x$. Define $u_1 := 2f + x$ and $u_2 := ae + bf + cx$, where $a := \frac{\lambda}{1-\lambda^{-1}\mu}$, $b := \frac{(1-\lambda^{-1}\mu)^2 - (\lambda+\mu)^2}{2\lambda(1-\lambda^{-1}\mu)}$, and $c := \frac{-\lambda-\mu}{1-\lambda^{-1}\mu}$. One can then check that the following hold:

$$(u_1, u_1) = (u_2, u_2) = 1, \quad (v, u_1) = (u_1, u_2) = \lambda, \quad (u_2, w) = -\lambda.$$

Therefore $\langle v \rangle - \langle u_1 \rangle - \langle u_2 \rangle - \langle w \rangle$ is a path of length 3 and hence $d(\alpha, \beta) \leq 3$. It follows that $\text{diam}(\Gamma_{\pm\lambda}^s) \leq 3$. $\square$

Proposition 4.3.18. *Let $q \geq 17$. Then $\text{diam}(\Gamma_0^s) \leq 3$.*

Proof. Let $\{e, f, x\}$ be the standard basis and let $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$ be two distinct elements of X_s . If $(v, w) = 0$, then $d(\alpha, \beta) = 1$. Suppose $(v, w) = \mu$, where $\mu \in \mathbb{F}_q^*$. Without loss of generality, we may assume that $v = x$ and $w = \frac{1}{2}(1 - \mu)e + (1 + \mu)f + \mu x$. We will show that $d(\alpha, \beta) \leq 3$ by proving the existence of a path of length 3 between α and β . Observe that $\alpha - \langle u_1 \rangle$ is an edge if and only if $u_1 = de + \frac{1}{2d}f$, for some $d \in \mathbb{F}_q^*$. Let $u_2 := c_1e + c_2f + c_3x$ where $c_i \in \mathbb{F}_q$. Then $\alpha - \langle u_1 \rangle - \langle u_2 \rangle - \beta$ is a path of length 3 if and only if

$$2c_1c_2 + c_3^2 = 1, \tag{4.2}$$

$$dc_2 + \frac{c_1}{2d} = 0, \tag{4.3}$$

$$c_1(1 + \mu) + \frac{1}{2}c_2(1 - \mu) + c_3\mu = 0. \tag{4.4}$$

By (4.3) we have $c_1 = -2d^2c_2$. Substituting this into (4.4) and rearranging for c_3 we obtain

$$c_3 = \frac{(4d^2 - 1 + (4d^2 + 1)\mu)c_2}{2\mu}.$$

Now substituting the expressions obtained for c_1 and c_3 into (4.2) we see that $c_2^2 f(d, \mu) = 4\mu^2$, where

$$f(d, \mu) := (4d^2 - 1)(4d^2(\mu + 1)^2 - (\mu - 1)^2).$$

We conclude that there exists a path of length 3 between α and β if and only if there exists $d \in \mathbb{F}_q^*$ such that $f(d, \mu)$ is a square in $\mathbb{F}_q^*$. If $\mu = -1$, then $f(d, \mu) = 4(1 - 4d^2)$. Now the number of solutions $(a, b) \in (\mathbb{F}_q^*)^2$ to the equation $a^2 + b^2 = 1$ is at least $q - 5$ (see Lemma A.7 in Appendix A). Since $q > 5$ we can pick such a solution (a, b) and let $d = 2^{-1}a$. Then $f(d, \mu) = 4b^2$, a non-zero square. If $\mu \neq -1$ then $f(d, \mu)$ is a non-zero square if and only if $(4d^2 - 1)(4d^2 - (\frac{\mu-1}{\mu+1})^2)$ is a non-zero square. Define $y := 2d$ and $a := \frac{\mu-1}{\mu+1}$. Then, in order to conclude the proof it suffices to show that for each $a \in \mathbb{F}_q \setminus \{\pm 1\}$ there exists $y \in \mathbb{F}_q^*$ such that $(y^2 - 1)(y^2 - a^2)$ is a square in $\mathbb{F}_q^*$. Provided that $q \geq 17$, the latter can be shown using a number-theoretical argument which can be found as Lemma A.1 in Appendix A. $\square$

So far we have been analysing the orbital graphs of $(\text{SO}_3(q), X_s)$. Now we will analyse the orbital graphs of $(\Omega_3(q), X_s)$. We begin by stating some results concerning the sizes of the suborbits of $(\text{SO}_3(q), X_s)$ and $(\Omega_3(q), X_s)$.

Proposition 4.3.19. *Let $\{e, f, x\}$ be the standard basis and let $\Delta_{\pm\lambda}^s(\alpha)$ be the suborbit of $(\text{SO}_3(q), X_s)$ corresponding to the orbital $\Delta_{\pm\lambda}^s$, where $\alpha := \langle x \rangle$. Then $|\Delta_{\pm 1}^s(\alpha)| = 2(q - 1)$ and $|\Delta_0^s(\alpha)| = \frac{q-1}{2}$.*

Proof. Recall that

$$\Delta_{\pm\lambda}^s(\alpha) = \{\beta \in X_s : (\alpha, \beta) \in \Delta_{\pm\lambda}^s\}.$$

Now since $\langle x \rangle^\perp$ is non-degenerate, we have $V = \langle x \rangle \perp \langle x \rangle^\perp$, and thus

$$\Delta_{\pm\lambda}^s(\alpha) = \{\langle \pm\lambda x + w \rangle \in X_s : w \in \langle x \rangle^\perp \setminus \{0\}, (w, w) = 1 - \lambda^2\}.$$

Therefore the size of $\Delta_{\pm 1}^s(\alpha)$ is the number of $w \in \langle x \rangle^\perp \setminus \{0\}$ with $(w, w) = 0$, since each such w gives a unique element of $\Delta_{\pm 1}^s(\alpha)$ of the form $\langle x + z \rangle$ for $z \in \langle w \rangle^\perp \setminus \{0\}$. Suppose w is such an element. Since $\langle x \rangle^\perp = \langle e, f \rangle$, writing $w = ae + bf$, where $a, b \in \mathbb{F}_q$ and a and b are not both zero, we see that $(w, w) = 0$ if and only if $ab = 0$. If $a = 0$, then there are $q - 1$ values for b and vice versa. So the number of pairs (a, b) for which $(w, w) = 0$ is $2(q - 1)$. Therefore $|\Delta_{\pm 1}^s(\alpha)| = 2(q - 1)$.

The size of $\Delta_0^s(\alpha)$ is half the number of $w \in \langle x \rangle^\perp \setminus \{0\}$ with $(w, w) = 1$, since w and $-w$ generate the same subspace. Suppose w is such an element. Writing $w = ae + bf$, where $a, b \in \mathbb{F}_q$ and a and b are not both zero, we see that $(w, w) = 1$ if and only if $2ab = 1$. There are $q - 1$ such values for a and each one determines the value of b . So the number of pairs (a, b) for which $(w, w) = 1$ is $q - 1$. Therefore $|\Delta_0^s(\alpha)| = \frac{q-1}{2}$. $\square$

Proposition 4.3.20 (Tables 2.3.1, 2.2.1 and 2.2.2 in [13]). *The sizes of the suborbits of $(\mathrm{SO}_3(q), X_s)$ and $(\Omega_3(q), X_s)$ are given in Tables 4.3, 4.4, and 4.5.*

Suborbit size	1	$q - 1$	$\frac{q-1}{2}$	$2(q - 1)$
Number of suborbits	1	$\frac{q-3}{2}$	1	1

Table 4.3: Suborbits of $(\mathrm{SO}_3(q), X_s)$

Suborbit size	1	$\frac{q-1}{4}$	$\frac{q-1}{2}$	$q - 1$
Number of suborbits	1	2	$\frac{q-5}{2}$	$\frac{q+7}{4}$

Table 4.4: Suborbits of $(\Omega_3(q), X_s)$, where $q \equiv 1 \pmod{4}$

Suborbit size	1	$\frac{q-1}{2}$	$q-1$
Number of suborbits	1	$\frac{q-1}{2}$	$\frac{q+5}{4}$

Table 4.5: Suborbits of $(\Omega_3(q), X_s)$, where $q \equiv 3 \pmod{4}$

Recall that $\Omega_3(q)$ is a subgroup of $\text{SO}_3(q)$ of index 2 and hence we can use Proposition 2.1.5 to obtain information about the suborbits of $(\Omega_3(q), X_s)$. In what follows, we will use the fact that $-1 \in \mathbb{F}_q$ is a square if and only if $q \equiv 1 \pmod{4}$ (see Lemma A.6 in Appendix A for a proof).

Proposition 4.3.21. *Let $S := \Omega_3(q)$. The suborbit $\Delta_{\pm 1}^s(\alpha)$ from Proposition 4.3.19 splits into two suborbits $\Delta_{\pm 1}^{s1}(\alpha)$ and $\Delta_{\pm 1}^{s2}(\alpha)$ of (S, X_s) , which are self-paired if and only if $q \equiv 1 \pmod{4}$, and are otherwise paired with each other.*

Proof. Let $\{e, f, x\}$ be the standard basis. Firstly note that $\Delta_{\pm 1}^s(\alpha) = \beta^{G_\alpha}$, where $\beta := \langle e + x \rangle$ and $G := \text{SO}_3(q)$. Using the Orbit-Stabiliser property and Proposition 4.3.19, we have $|G_{\alpha\beta}| = 1$. Hence $|G_{\alpha\beta} : G_{\alpha\beta} \cap S| = 1$ and so the suborbit $\Delta_{\pm 1}^s(\alpha)$ splits by Proposition 2.1.5. This proves the first claim.

By relabelling, we may assume that $\Delta_{\pm 1}^{s1}(\alpha) = \beta^{S_\alpha}$. Now $\Delta_{\pm 1}^{s1}(\alpha)$ is self-paired if and only if there exists $g \in S$ such that $\alpha^g = \beta$ and $\beta^g = \alpha$. Suppose $g \in S$ such that the latter holds. Note that $g^2 \in G_{\alpha\beta} = 1$. Now $\alpha = \langle x \rangle$ and thus $\alpha^g = \beta$ implies $x^g = a(e + x)$ for some $a \in \mathbb{F}_q$. Moreover,

$$1 = (x, x) = (x^g, x^g) = (a(e + x), a(e + x)) = a^2$$

implies $a = \pm 1$. Similarly we can deduce $(e + x)^g = bx$, where $b = \pm 1$. If $(a, b) = (1, -1)$ or $(-1, 1)$, then simple calculations show that $e^{g^2} = -e$ which contradicts the fact that $g^2 = 1$, hence these cases cannot occur. Now suppose $(a, b) = (-1, -1)$. Then $e^g = e$. Write $f^g = c_1e + c_2f + c_3x$, where

$c_i \in \mathbb{F}_q$. Then we have

$$g = \begin{pmatrix} 1 & 0 & 0 \\ c_1 & c_2 & c_3 \\ -1 & 0 & -1 \end{pmatrix}, \quad g^2 = \begin{pmatrix} 1 & 0 & 0 \\ c_1 + c_1c_2 - c_3 & c_2^2 & c_2c_3 - c_3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Now $\det(g) = 1$ implies $c_2 = -1$, and $g^2 = 1$ implies $c_3 = 0$. Therefore $f^g = c_1e - f$. Finally, $(f^g, f^g) = (f, f) = 0$ implies $c_1 = 0$ which gives

$$1 = (e, f) = (e^g, f^g) = (e, -f) = -1.$$

Hence this case cannot occur. Therefore $(a, b) = (1, 1)$. In this case $e^g = -e$. Writing f^g as in the previous case, we obtain

$$g = \begin{pmatrix} -1 & 0 & 0 \\ c_1 & c_2 & c_3 \\ 1 & 0 & 1 \end{pmatrix}, \quad g^2 = \begin{pmatrix} 1 & 0 & 0 \\ -c_1 + c_1c_2 + c_3 & c_2^2 & c_3c_2 + c_3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Now $\det(g) = 1$ implies $c_2 = -1$, and $g^2 = 1$ implies $c_3 = 2c_1$. Thus $f^g = c_1e - f + 2c_1x$. Finally, since

$$0 = (f, f) = (f^g, f^g) = (c_1e - f + 2c_1x, c_1e - f + 2c_1x) = 2c_1(2c_1 - 1),$$

we must have either $c_1 = 0$ or $c_1 = 1/2$. If $c_1 = 0$, then

$$0 = (f, x) = (f^g, x^g) = (-f, e + x) = -1,$$

which is a contradiction. Hence $c_1 = 1/2$ and

$$g = \begin{pmatrix} -1 & 0 & 0 \\ 1/2 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in G.$$

We claim that $g \in S$ if and only if $q \equiv 1 \pmod{4}$. Now $g \in S$ if and only if the spinor norm of g is equal to 1. We use Proposition 1.6.11 from [3] to calculate the spinor norm of g as follows. Define the following matrices:

$$A := I_3 - g = \begin{pmatrix} 2 & 0 & 0 \\ -1/2 & 2 & -1 \\ -1 & 0 & 0 \end{pmatrix}, B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, F := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

By Proposition 1.6.11 in [3], the spinor norm of g is 1 if and only if $\det(BAFB^T)$ is a square in $\mathbb{F}_q^*$ and -1 otherwise. Now

$$BAFB^T = \begin{pmatrix} 0 & 2 \\ 2 & -1/2 \end{pmatrix},$$

and $\det(BAFB^T) = -4$ is a square if and only if $q \equiv 1 \pmod{4}$. Therefore $\Delta_{\pm 1}^1(\alpha)$ is self-paired if and only if $q \equiv 1 \pmod{4}$.

Finally, we deduce from Proposition 4.3.20 that all but two of the suborbits of (S, X_s) of size $q - 1$ are also suborbits of (G, X_s) and hence self-paired. We use this to conclude that $\Delta_{\pm 1}^{s1}(\alpha)$ and $\Delta_{\pm 1}^{s2}(\alpha)$ are either both self-paired or paired with each other. Hence $\Delta_{\pm 1}^{s2}(\alpha)$ is also self-paired if and only if $q \equiv 1 \pmod{4}$, and $\Delta_{\pm 1}^{s1}(\alpha)$ and $\Delta_{\pm 1}^{s2}(\alpha)$ are paired with each other if $q \equiv 3 \pmod{4}$. $\square$

Corollary 4.3.22. *If $q \equiv 3 \pmod{4}$, then $\Gamma_{\pm 1}^s$ is an orbital graph of (S, X_s) of diameter 2.*

Proof. Consider the orbital $\Delta_{\pm 1}^{s1}$ corresponding to the suborbit $\Delta_{\pm 1}^{s1}(\alpha)$ from Proposition 4.3.21. The orbital graph corresponding to this orbital is the undirected graph with vertex set X_s and with edges $\{x, y\}$ where $(x, y) \in \Delta_{\pm 1}^{s1}$. The edge-set of this graph is trivially contained in the edge-set of $\Gamma_{\pm 1}^s$. However if $q \equiv 3 \pmod{4}$, then using Proposition 4.3.21 we deduce that the reverse inclusion also holds, and therefore the edge-sets are equal and the or-

bital graph corresponding to $\Delta_{\pm 1}^{s1}$ is $\Gamma_{\pm 1}^s$, which has diameter 2 by Proposition 4.3.15. $\square$

Now let G be an almost simple group with $\text{soc}(G) \cong \Omega_3(q) =: S$. Recall from Proposition 4.3.8(1) that $\text{Aut}(S) = \langle S, \dot{\delta}, \dot{\phi} \rangle$. In order to determine the orbitals of (G, X_s) and (G, X_n) we need to determine the action of $\dot{\delta}$ and $\dot{\phi}$ on the orbitals of (S, X_s) and (S, X_n) .

Remark 4.3.23. Recall that $G := \text{SO}_3(q) \cong \langle S, \dot{\delta} \rangle$ by Proposition 4.3.8(2), where $S := \Omega_3(q)$ and thus the action of $\dot{\delta}$ on the orbitals of (S, X_l) (where $l \in \{s, n\}$) is determined by Proposition 2.1.5. In other words, if the orbital Δ of (G, X_l) splits into two orbitals Δ_1 and Δ_2 of (S, X_l) , then $\dot{\delta}$ swaps them, and if Δ remains an orbital of (S, X_l) , then $\dot{\delta}$ fixes it. Therefore it only remains to determine the action of $\dot{\phi}$ on the orbitals of (S, X_l) . For an orbital Δ the action of $\dot{\phi}$ on Δ will be denoted by $\Delta^{\dot{\phi}}$.

Proposition 4.3.24. *Let $l \in \{s, n\}$ and let $\Delta_{\pm \lambda}^l$ be an orbital of $(\text{SO}_3(q), X_l)$, where q is a power of the prime p . Then $(\Delta_{\pm \lambda}^l)^{\dot{\phi}} = \Delta_{\pm \lambda^p}^l$.*

Proof. Let $\{e, f, x\}$ be the standard basis. Recall from Remark 4.3.6 that for $u, v \in V$, we have

$$(u^\phi, v^\phi) = (u, v)^p. \quad (4.5)$$

Now fix l and suppose $(\langle u \rangle, \langle v \rangle) \in \Delta_{\pm \lambda^p}^l$, where $(u, u) = (v, v) = \alpha$ and $(u, v) = \pm \lambda^p \alpha$ (recall that α is 1 if $l = s$ and the non-square γ if $l = n$). Write

$$u = u_1 e + u_2 f + u_3 x, \quad v = v_1 e + v_2 f + v_3 x,$$

for some $u_i, v_i \in \mathbb{F}_q$. Now, define

$$u' := u_1^{1/p} e + u_2^{1/p} f + u_3^{1/p} x, \quad v' := v_1^{1/p} e + v_2^{1/p} f + v_3^{1/p} x,$$

and pick $z \in \mathbb{F}_q$ such that $z^2 = \alpha^{-1/p} \alpha$. Then using (4.5) one can check that $(\langle zu' \rangle, \langle zv' \rangle) \in \Delta_{\pm \lambda}^l$ and $(\langle zu' \rangle, \langle zv' \rangle)^{\dot{\phi}} = (\langle u \rangle, \langle v \rangle)$. This proves that

$\Delta_{\pm\lambda^p}^l \subseteq (\Delta_{\pm\lambda}^l)^\phi$. For the converse, suppose that $(\langle u \rangle, \langle v \rangle) \in \Delta_{\pm\lambda}^l$, where $(u, u) = (v, v) = \alpha$ and $(u, v) = \pm\lambda\alpha$. Pick $z \in \mathbb{F}_q$ such that $z^2 = \alpha^{-p}\alpha$. Then using (4.5) one can check that

$$(\langle u \rangle, \langle v \rangle)^\phi = (\langle u^\phi \rangle, \langle v^\phi \rangle) = (\langle zu^\phi \rangle, \langle zv^\phi \rangle) \in \Delta_{\pm\lambda^p}^l.$$

This proves that $(\Delta_{\pm\lambda}^l)^\phi \subseteq \Delta_{\pm\lambda^p}^l$. $\square$

We will need one final result before we can determine the action of $\dot{\phi}$ on the orbitals of $(\Omega_3(q), X_l)$ for $l \in \{s, n\}$.

Lemma 4.3.25. *Let (A, X) , (G, X) and (S, X) be three permutation groups with $S \leq G \leq A$, and suppose S has index 2 in G . Suppose also that $f \in A_\alpha$ and the suborbit β^{G_α} of (G, X) splits in (S, X) . Then $(\beta^f)^{G_\alpha}$ also splits in (S, X) .*

Proof. Since S has index 2 in G , by Proposition 2.1.5, the suborbit $(\beta^f)^{G_\alpha}$ splits if and only if $G_{\alpha\beta f} = S_{\alpha\beta f}$. Now it is straightforward to verify that $G_{\alpha\beta f} = f^{-1}G_{\alpha\beta}f$ and $S_{\alpha\beta f} = f^{-1}S_{\alpha\beta}f$. Then since β^{G_α} splits, we have $G_{\alpha\beta f} = f^{-1}G_{\alpha\beta}f = f^{-1}S_{\alpha\beta}f = S_{\alpha\beta f}$, which implies that $(\beta^f)^{G_\alpha}$ also splits in (S, X) . $\square$

Proposition 4.3.26. *Let $S := \Omega_3(q)$. Suppose that the orbital $\Delta_{\pm\lambda}^s$ splits in (S, X_s) into two orbitals $\Delta_{\pm\lambda}^{s_i}$ ($i = 1, 2$). Then $\Delta_{\pm\lambda}^{s_i \dot{\phi}} = \Delta_{\pm\lambda^p}^{s_i}$.*

Proof. We have $\Delta_{\pm\lambda}^s = \Delta_{\pm\lambda}^{s_1} \cup \Delta_{\pm\lambda}^{s_2}$. Hence, by Proposition 4.3.24,

$$\Delta_{\pm\lambda^p}^s = (\Delta_{\pm\lambda}^{s_1} \cup \Delta_{\pm\lambda}^{s_2})^{\dot{\phi}} = \Delta_{\pm\lambda}^{s_1 \dot{\phi}} \cup \Delta_{\pm\lambda}^{s_2 \dot{\phi}}.$$

Let $\{e, f, x\}$ be the standard basis. If $\Delta_{\pm\lambda}^s$ corresponds to the suborbit β^{G_α} , where $\alpha := \langle x \rangle$ and $G := \text{SO}_3(q)$, then by Proposition 4.3.24, $\Delta_{\pm\lambda^p}^s$ corresponds to the suborbit $(\beta^{\dot{\phi}})^{G_\alpha}$. Now since $\Delta_{\pm\lambda}^s$ splits in (S, X_s) and $\dot{\phi}$ stabilises α , by Lemma 4.3.25 we have that $\Delta_{\pm\lambda^p}^s$ also splits in (S, X_s) , into

say $\Delta_{\pm\lambda^p}^{s1}$ and $\Delta_{\pm\lambda^p}^{s2}$. Therefore we obtain

$$\Delta_{\pm\lambda^p}^{s1} \cup \Delta_{\pm\lambda^p}^{s2} = \Delta_{\pm\lambda}^{s1} \dot{\phi} \cup \Delta_{\pm\lambda}^{s2} \dot{\phi}.$$

Since all four sets in the unions above are orbitals of (S, X_s) , any two of them must either be disjoint or equal. However, $\Delta_{\pm\lambda}^{si} \dot{\phi}$ cannot be disjoint to $\Delta_{\pm\lambda^p}^{sj}$ for both $j = 1$ and $j = 2$. Therefore $\Delta_{\pm\lambda}^{si} \dot{\phi} = \Delta_{\pm\lambda^p}^{sj}$, either for $j = 1$ or for $j = 2$. If $\lambda \neq \pm\lambda^p$, then by relabelling if necessary, we may assume that $j = i$. Now suppose $\lambda = \pm\lambda^p$. Then either $\dot{\phi}$ fixes $\Delta_{\pm\lambda}^{s1}$ and $\Delta_{\pm\lambda}^{s2}$ or swaps them. We claim that the former holds. To see this, if $\lambda = \lambda^p$, then define $\beta := \langle \lambda x + c_1 e + c_2 f \rangle$ where $c_1 := 2^{-1}$ and $c_2 := 1 - \lambda^2$, and if $\lambda = -\lambda^p$ with $\lambda \neq 0$, then define $\beta = \langle -\lambda x + c_1 e + c_2 f \rangle$ where $c_1 := \lambda$ and $c_2 := \frac{1-\lambda^2}{2\lambda}$. Then $(\alpha, \beta) \in \Delta_{\pm\lambda}^s$ and $(\alpha, \beta)^{\dot{\phi}} = (\alpha, \beta)$, and hence $\dot{\phi}$ cannot swap $\Delta_{\pm\lambda}^{s1}$ and $\Delta_{\pm\lambda}^{s2}$. $\square$

In the next result, we apply Proposition 4.3.26 with a specific value of λ .

Corollary 4.3.27. *Let $S := \Omega_3(q)$. The orbital Δ_0^s splits into two orbitals Δ_0^{s1} and Δ_0^{s2} of (S, X_s) if and only if $q \equiv 1 \pmod{4}$. In the case where it splits, we have $\Delta_0^{si\dot{\phi}} = \Delta_0^{si}$ for $i = 1, 2$.*

Proof. By Proposition 4.3.20 we have that $(\text{SO}_3(q), X_s)$ has a unique suborbit of size $\frac{q-1}{2}$ and by Proposition 4.3.19 this suborbit must be the one corresponding to Δ_0^s . Now Δ_0^s splits in (S, X_s) if and only if (S, X_s) has two suborbits of size $\frac{q-1}{4}$ each (see Remark 2.1.6). By Proposition 4.3.20, this is the case if and only if $q \equiv 1 \pmod{4}$. The last assertion follows from Proposition 4.3.26. $\square$

Remark 4.3.28. For $\Delta_{\pm\lambda}^{si}$ as in Proposition 4.3.26, we will denote the corresponding orbital graph by $\Gamma_{\pm\lambda}^{si}$. Note that the vertex set of $\Gamma_{\pm\lambda}^{si}$ is equal to the vertex set of $\Gamma_{\pm\lambda}^s$ but the edge set is only a subset, hence we have that $\text{diam}(\Gamma_{\pm\lambda}^{si}) \geq \text{diam}(\Gamma_{\pm\lambda}^s)$.

We can now prove Theorem 4.3.1.

Proof of Theorem 4.3.1. Let G and X be as in the statement of the theorem. By Proposition 4.1.2(1) and Corollary 4.3.13, we may suppose $\text{soc}(G) = \Omega_3(q)$ and $X = X_s$. To prove the first part of the theorem, it suffices to show that (G, X) has an orbital graph of diameter at least 3. Indeed, by Proposition 4.3.24 and Corollary 4.3.27, either Γ_0^s or Γ_0^{si} (for some $i = 1, 2$) is an orbital graph of (G, X) . Now $\text{diam}(\Gamma_0^{si}) \geq \text{diam}(\Gamma_0^s)$ (see Remark 4.3.28), and by Proposition 4.3.16 we have $\text{diam}(\Gamma_0^s) \geq 3$. This proves part 1. Now suppose that $q \equiv 3 \pmod{4}$. By Corollary 4.3.22, $\Gamma_{\pm 1}^s$ is an orbital graph of $(\Omega_3(q), X)$ of diameter 2, and by Proposition 4.3.24, it is also an orbital graph of (G, X) . This proves part 2. The last assertion concerning $G = \text{SO}_3(q)$ follows from Propositions 4.3.15, 4.3.17 and 4.3.18. $\square$

It now remains to prove Theorem 4.3.2. To do this, we now prove some results concerning the orbitals $\Delta_{\pm\lambda}^n$. Recall that X_n is the set of 1-dimensional subspaces $\langle v \rangle$ such that (v, v) is a non-square, and without loss of generality, we may assume $(v, v) = \gamma$, where γ is a fixed non-square in $\mathbb{F}_q$.

Proposition 4.3.29 (Table 2.3.2 in [13]). *The sizes of the suborbits of $(\text{SO}_3(q), X_n)$ are given in Table 4.6.*

Suborbit size	1	$\frac{q+1}{2}$	$q+1$
Number of suborbits	1	1	$\frac{q-3}{2}$

Table 4.6: Suborbits of $(\text{SO}_3(q), X_n)$

Proposition 4.3.30. *Let $q \geq 11$. Then $\text{diam}(\Gamma_0^n) \geq 3$.*

Proof. Note that the condition $q \geq 11$ ensures that Γ_0^n is connected. Let $\{e, f, x\}$ be the standard basis. Define $v := e + \frac{\gamma}{2}f$. Choose $\beta \in \mathbb{F}_q^*$ such that $\beta^2 \neq \pm 1$, and define $w := \beta e + \frac{\gamma}{2\beta}f$. Observe that $(v, v) = (w, w) = \gamma$, and so $\langle v \rangle, \langle w \rangle \in X_n$. Moreover, since $\beta \neq 1$ we have $v \neq w$, and since $\gamma \neq 0$ and

$1 + \beta^2 \neq 0$, we have

$$(v, w) = \frac{\gamma}{2\beta} + \frac{\gamma\beta}{2} = \frac{\gamma(1 + \beta^2)}{2\beta} \neq 0.$$

Therefore $d(\langle v \rangle, \langle w \rangle) \geq 2$. Suppose that $d(\langle v \rangle, \langle w \rangle) = 2$ and $\langle y \rangle$ is a common neighbour of $\langle v \rangle$ and $\langle w \rangle$. Write $y = ae + bf + cx$, where $a, b, c \in \mathbb{F}_q$. Then $(y, y) = \gamma$, $(v, y) = 0$ and $(w, y) = 0$ imply

$$2ab + c^2 = \gamma \tag{4.6}$$

$$b + \frac{a\gamma}{2} = 0 \tag{4.7}$$

$$\frac{a\gamma}{2\beta} + b\beta = 0. \tag{4.8}$$

Using (4.7) and (4.8) to eliminate γ , we obtain $b(1 - \beta^2) = 0$. Since $\beta^2 \neq 1$, this implies $b = 0$. Now substituting $b = 0$ in (4.6), we obtain $c^2 = \gamma$, which is a contradiction since γ is a non-square. Therefore $d(\langle v \rangle, \langle w \rangle) \geq 3$, from which the result follows. $\square$

Proposition 4.3.31. *Let $\{e, f, x\}$ be the standard basis and let $\Delta_{\pm\lambda}^n(\alpha)$ be the suborbit of $(\text{SO}_3(q), X_n)$ corresponding to the orbital $\Delta_{\pm\lambda}^n$, where $\alpha := \langle e + \frac{\gamma}{2}f \rangle$. Then $|\Delta_0^n(\alpha)| = \frac{q+1}{2}$.*

Proof. Recall that

$$\Delta_{\pm\lambda}^n(\alpha) = \{\beta \in X_n : (\alpha, \beta) \in \Delta_{\pm\lambda}^n\}.$$

Now since α is non-degenerate, we have $V = \alpha \perp \alpha^\perp$, and thus

$$\Delta_{\pm\lambda}^n(\alpha) = \left\{ \left\langle \pm\lambda \left(e + \frac{\gamma}{2}f \right) + w \right\rangle \in X_n : w \in \alpha^\perp \setminus \{0\}, (w, w) = \gamma(1 - \lambda^2) \right\}.$$

Therefore the size of $\Delta_0^n(\alpha)$ is the half the number of $w \in \alpha^\perp \setminus \{0\}$ with $(w, w) = \gamma$, since w and $-w$ generate the same subspace. Suppose w is such an element. Since $\alpha^\perp = \langle e - \frac{\gamma}{2}f, x \rangle$, writing $w = a(e - \frac{\gamma}{2}f) + bx$, where

$a, b \in \mathbb{F}_q$ and a and b are not both zero, we see that $(w, w) = \gamma$ if and only if $b^2 - a^2\gamma = \gamma$. The number of solutions (a, b) to this equation is $q + 1$ (see Lemma A.10 in Appendix A), from which the result follows. $\square$

Now it turns out that if $q \equiv 3 \pmod{4}$, then $(\Omega_3(q), X_n)$ has precisely two suborbits of size $\frac{q+1}{4}$ (see Table 2.2.5 in [13]), and thus in this case Δ_0^n splits into two orbitals of $(\Omega_3(q), X_n)$. Next, we would like to determine the action of $\dot{\phi}$ on these two orbitals.

Proposition 4.3.32. *Suppose the orbital Δ_0^n splits in $(\Omega_3(q), X_n)$ into two orbitals Δ_0^{ni} ($i = 1, 2$). Then $\Delta_0^{ni\dot{\phi}} = \Delta_0^{ni}$.*

Proof. Suppose Δ_0^n splits in $(\Omega_3(q), X_n)$. Then the corresponding suborbit (which has size $\frac{q+1}{2}$ by Proposition 4.3.31) also splits into two suborbits, of size $\frac{q+1}{4}$ each. Thus $q \equiv 3 \pmod{4}$. Write $q = p^r$ for some prime p . Then we have that r is odd (and $p \equiv 3 \pmod{4}$). Recall that r is the order of $\dot{\phi}$, and thus $\dot{\phi}$ has odd order. Now by Proposition 4.3.24, we have

$$\Delta_0^{n1} \cup \Delta_0^{n2} = \Delta_0^n = \Delta_0^{n1\dot{\phi}} \cup \Delta_0^{n2\dot{\phi}}.$$

Thus $\Delta_0^{n1\dot{\phi}} = \Delta_0^{nj\dot{\phi}}$, for either $j = 1$ or 2 , i.e. $\dot{\phi}$ either fixes Δ_0^{ni} for $i = 1, 2$ or swaps them. If the latter holds, then $\dot{\phi}$ must have even order which is a contradiction. Hence $\dot{\phi}$ fixes Δ_0^{ni} for $i = 1, 2$. $\square$

For Δ_0^{ni} as in Proposition 4.3.32, we will denote the corresponding orbital graph by Γ_0^{ni} . The next aim is to prove that for sufficiently large values of q , all orbital graphs of $(\text{SO}_3(q), X_n)$ have diameter at least 3. To do this we take a different approach as follows.

Since all non-degenerate quadratic forms of dimension 3 are similar, we will now assume now that the underlying vector space V has basis $\{v_1, v_2, v_3\}$ where $(v_i, v_j) := \delta_{ij}$ for all i, j except $i = j = 2$, and $(v_2, v_2) := \beta$ where β is a non-square if $q \equiv 1 \pmod{4}$ and a non-zero square if $q \equiv 3 \pmod{4}$. For the remainder of this section, we will refer to this basis as *the* orthogonal basis.

Define Y_s to be the set of 1-dimensional subspaces $\langle v \rangle$ of V such that (v, v) is a square; without loss of generality, we may assume $(v, v) = 1$. We now analyse the natural action of $\text{SO}_3(q)$ and $\Omega_3(q)$ on Y_s .

Lemma 4.3.33. *We have $|Y_s| = \frac{q(q-1)}{2}$.*

Proof. As in the proof of Lemma 4.3.10, we have that $|Y_s|$ is half the number of vectors v such that $(v, v) = 1$. Let $\{v_1, v_2, v_3\}$ be the orthogonal basis and write $v = av_1 + bv_2 + cv_3$, where $a, b, c \in \mathbb{F}_q$. Then $(v, v) = a^2 + b^2\beta + c^2$. First suppose that β is a square, i.e. $q \equiv 3 \pmod{4}$. If $c = \pm 1$, then there are 2 solutions $(a, b, c) = (0, 0, \pm 1)$ to $(v, v) = 1$. If $c \neq \pm 1$ then there are $q + 1$ solutions to $(v, v) = 1$ (by Lemma A.7 if $1 - c^2$ is a square, and by Lemma A.10 if $1 - c^2$ is a non-square). Hence, the number of vectors v such that $(v, v) = 1$, is $(q - 2)(q + 1) + 2 = q(q - 1)$, and the result follows. Now suppose that β is a non-square, i.e. $q \equiv 1 \pmod{4}$. As above, if $c = \pm 1$, then there are 2 solutions $(a, b, c) = (0, 0, \pm 1)$ to $(v, v) = 1$. Moreover, if $c \neq \pm 1$ then there are again $q + 1$ solutions to $(v, v) = 1$ (this can be shown using similar arguments as in the proof of Lemma A.7 for both of the cases where $1 - c^2$ is a square and a non-square). Thus the result follows in this case too. $\square$

Remark 4.3.34. Note that since $|Y_s| = \frac{q(q-1)}{2}$, the set Y_s is equal to the set X_s from earlier on.

It can be shown in a similar way to the proofs of Propositions 4.3.11 and 4.3.12, that $\text{SO}_3(q)$ and $\Omega_3(q)$ act transitively on Y_s . Furthermore, we have the following result.

Proposition 4.3.35. *Let $G := \text{SO}_3(q)$. For $\alpha \in Y_s$, we have $G_\alpha = O_2^-(q)$.*

Proof. Let $\{v_1, v_2, v_3\}$ be the orthogonal basis. We have $\langle v_3 \rangle \in Y_s$, and therefore it suffices to show that $G_{\langle v_3 \rangle} = O_2^-(q)$. Since $\langle v_3 \rangle$ is non-degenerate, we have $V = \langle v_3 \rangle \perp \langle v_3 \rangle^\perp$ and thus $G_{\langle v_3 \rangle} = G_{\langle v_3 \rangle^\perp}$. Now, for $a, b \in \mathbb{F}_q$,

$$(av_1 + bv_2, av_1 + bv_2) = a^2 + b^2\beta, \quad (4.9)$$

Since $-\beta$ is a non-square, the right hand side of (4.9) is non-zero, and hence $\langle v_3 \rangle^\perp = \langle v_1, v_2 \rangle$ does not contain a 1-dimensional totally singular subspace. Thus $G_{\langle v_3 \rangle} = G_{\langle v_3 \rangle^\perp} \leq O_2^-(q)$ (see Proposition 2.5.4(i) in [14]). Now $|Y_s| = \frac{q(q-1)}{2}$ and thus by using the Orbit-Stabiliser property we have $|G_{\langle v_3 \rangle}| = |O_2^-(q)|$ which implies $G_{\langle v_3 \rangle} = O_2^-(q)$. $\square$

The following result can be proved in a similar way to Corollary 4.3.12.

Corollary 4.3.36. *Let $S := \Omega_3(q)$. For $\alpha \in Y_s$, we have $S_\alpha \cong D_{q+1}$.*

By Corollary 4.3.36, in order to analyse the action of $\text{PSL}_2(q)$ on cosets of its maximal subgroup D_{q+1} , it suffices to analyse the action of $\Omega_3(q)$ on Y_s . The following result can be proved in a similar way to Proposition 4.3.14.

Proposition 4.3.37. *The non-diagonal orbitals of $(\text{SO}_3(q), Y_s)$ are*

$$\Delta_{\pm\lambda} := \{(\langle v \rangle, \langle w \rangle) \in Y_s \times Y_s : (v, v) = (w, w) = 1, (v, w) = \pm\lambda\},$$

where $\lambda \in \mathbb{F}_q \setminus \{\pm 1\}$.

Let $\Gamma_{\pm\lambda}$ denote the orbital graph corresponding to the orbital $\Delta_{\pm\lambda}$ from Proposition 4.3.37.

Proposition 4.3.38. *Let $q > 13$. For all $\lambda \neq 0, \pm 1$, we have $\text{diam}(\Gamma_{\pm\lambda}) \geq 3$.*

Proof. Let $\{v_1, v_2, v_3\}$ be the orthogonal basis and define $x := \langle v_1 \rangle \in Y_s$. We will show that for $q > 13$, there exists $y \in Y_s$ such that $d(x, y) \geq 3$. We start by considering the following two cases:

$q \equiv 1 \pmod{4}$: Define $y := \langle w \rangle \in Y_s$ where $w := av_1 + bv_3$ with $a, b \in \mathbb{F}_q$. Suppose $d(x, y) \leq 2$ for all $a, b \in \mathbb{F}_q$. Without loss of generality, we may assume $(w, w) = 1$, and so we must have

$$a^2 + b^2 = 1. \tag{4.10}$$

Now $d(x, y) = 1$ if and only if $b \neq 0$ and $a = \pm\lambda$. Also $d(x, y) = 2$ if and only if $b \neq 0$, $a \neq \pm\lambda$ and there exists a common neighbour $\langle u \rangle$ of x and y , i.e. $u = cv_1 + dv_2 + ev_3$ where $c, d, e \in \mathbb{F}_q$ and

$$c^2 + \beta d^2 + e^2 = 1 \quad (4.11)$$

$$c = \pm\lambda \quad (4.12)$$

$$ac + be = \pm\lambda. \quad (4.13)$$

Since $q \geq 9$, we can choose a solution (a, b) to (4.10) with $b \neq 0$ and $a \neq \pm\lambda$ (see Lemma A.7 in Appendix A). Then since $d(x, y) \neq 1$, we must have $d(x, y) = 2$. Combining (4.12) and (4.13), and using the fact that $b \neq 0$, we obtain

$$e = \frac{\pm\lambda(1-a)}{b}. \quad (4.14)$$

Substituting (4.14) into (4.11) and using $b^2 = 1 - a^2$ we obtain

$$\lambda^2 + \beta d^2 + \frac{\lambda^2(1-a)}{1+a} = 1.$$

Then rearranging, we obtain

$$\beta d^2 = \frac{1+a-2\lambda^2}{1+a}. \quad (4.15)$$

Now the solutions $(a, b) \neq (1, 0)$ of (4.10) can be written as

$$(a, b) = \left(\frac{u^2 - 1}{u^2 + 1}, \frac{-2u}{u^2 + 1} \right),$$

where $u \in \mathbb{F}_q$ and $u^2 + 1 \neq 0$ (see the proof of Lemma A.7 in Appendix A). Therefore by (4.15) we obtain

$$\beta d^2 = \frac{(1 - \lambda^2)u^2 - \lambda^2}{u^2},$$

where $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ since $a \neq -1, \pm\lambda$. Since the left-hand side is a non-square, we conclude that the numerator of the expression of the right-hand side must be a non-square for all $u \in \mathbb{F}_q$ with $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$.

$q \equiv 3 \pmod{4}$: Define $y := \langle w \rangle \in Y_s$ where $w := av_1 + bv_2$ with $a, b \in \mathbb{F}_q$. Suppose $d(x, y) \leq 2$ for all $a, b \in \mathbb{F}_q$. Using similar arguments to the previous case, we see that there exists $u = \pm\lambda v_1 + dv_2 + ev_3$ with $d, e \in \mathbb{F}_q$, such that

$$e^2 = \frac{1 + a - 2\lambda^2}{1 + a}.$$

Now as before, parametrising $a = \frac{u^2-1}{u^2+1}$, where $u \in \mathbb{F}_q$ with $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$, we obtain

$$e^2 = \frac{(1 - \lambda^2)u^2 - \lambda^2}{u^2}.$$

Therefore since the left-hand side is a square, we conclude that the numerator of the expression of the right-hand side must be a square for all $u \in \mathbb{F}_q$ with $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$.

In order to complete the proof, by the above, it suffices to prove the existence of elements u_1 for $q \geq 17$ and u_2 for $q \geq 19$ such that $u_i^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ and

$$(1 - \lambda^2)u_i^2 - \lambda^2$$

is a square for $i = 1$ and a non-square for $i = 2$. (Note that since $\lambda \neq 0$, the above expression is not trivially a square.) Indeed, such u_i can be shown to exist using a numerical argument which can be found as Lemma A.5 in Appendix A. $\square$

Proposition 4.3.39. *Let $\{v_1, v_2, v_3\}$ be the orthogonal basis and let $\Delta_0(\alpha)$ be the suborbit of $(\text{SO}_3(q), Y_s)$ corresponding to the orbital Δ_0 , where $\alpha := \langle v_3 \rangle$. Then $|\Delta_0(\alpha)| = \frac{q+1}{2}$.*

Proof. Recall that

$$\Delta_0(\alpha) = \{\beta \in Y_s : (\alpha, \beta) \in \Delta_0\}.$$

Now since $\langle v_3 \rangle$ is non-degenerate, we have $V = \langle v_3 \rangle \perp \langle v_3 \rangle^\perp$, and thus

$$\Delta_0(\alpha) = \{\langle w \rangle \in Y_s : w \in \langle v_3 \rangle^\perp \setminus \{0\}, (w, w) = 1\}.$$

Therefore the size of $\Delta_0(\alpha)$ is half the number of $w \in \langle v_3 \rangle^\perp \setminus \{0\}$ with $(w, w) = 1$, since w and $-w$ generate the same subspace. Suppose w is such an element. Since $\langle v_3 \rangle^\perp = \langle v_1, v_2 \rangle$, writing $w = av_1 + bv_2$, where $a, b \in \mathbb{F}_q$ and a and b are not both zero, we see that $(w, w) = 1$ if and only if $a^2 + \beta b^2 = 1$. Using similar arguments to the ones in Lemma A.7 in Appendix A, it can be seen that this equation has $q + 1$ solutions. So the number of pairs (a, b) for which $(w, w) = 1$ is $q + 1$. Therefore $|\Delta_0(\alpha)| = \frac{q+1}{2}$. $\square$

In the next result we return to the bilinear form specified by the standard basis $\{e, f, x\}$ and analyse the orbital graphs of the action of $\text{SO}_3(q)$ on the set X_n , defined previously.

Corollary 4.3.40. *Let $q > 13$. Then all orbital graphs of $(\text{SO}_3(q), X_n)$ have diameter at least 3.*

Proof. Let Γ be an orbital graph of the action and let Δ be the corresponding suborbit. By Proposition 4.3.29, the size of Δ is either $\frac{q+1}{2}$ or $q + 1$. If $|\Delta| = \frac{q+1}{2}$, then since there is a unique suborbit of this size, and $|\Delta_0^n| = \frac{q+1}{2}$ by Proposition 4.3.31, we have $\Gamma = \Gamma_0^n$ and the conclusion follows from Proposition 4.3.30. By Propositions 4.3.31 and 4.3.39, we have $|\Delta_0^n| = |\Delta_0|$. Hence if $|\Delta| = q + 1$, then we have $\text{diam}(\Gamma) = \text{diam}(\Gamma_{\pm\lambda})$ for some $\lambda \neq 0, \pm 1$. In this case, the conclusion follows from Proposition 4.3.38. $\square$

We can now prove Theorem 4.3.2.

Proof of Theorem 4.3.2. Let G and X be as in the statement of the theorem. By Proposition 4.1.2(1) and Corollary 4.3.13, we may suppose $\text{soc}(G) = \Omega_3(q)$ and $X = X_n$. To prove the first part of the theorem, it suffices to show that (G, X) has an orbital graph of diameter at least 3. Indeed, by Propositions 4.3.24 and 4.3.32, either Γ_0^n or Γ_0^{ni} (for some $i = 1, 2$) is an orbital

graph of (G, X) . Now $\text{diam}(\Gamma_0^{ni}) \geq \text{diam}(\Gamma_0^n)$ and by Proposition 4.3.30, we have $\text{diam}(\Gamma_0^n) \geq 3$. This proves part 1. Now suppose $G = \Omega_3(q)$ or $\text{SO}_3(q)$, and $q \geq 17$. By Corollary 4.3.40, all orbital graphs of $(\text{SO}_3(q), X)$ and hence of $(\Omega_3(q), X)$ have diameter at least 3. This proves part 2. $\square$

We conclude this section by presenting a conjecture which gives details of the orbital graph of diameter 2 in Conjecture 4.3.3. For orbital graphs $\Gamma_{\pm\lambda_1}^n, \dots, \Gamma_{\pm\lambda_l}^n$, by $\Gamma_{\pm\lambda_1}^n \cup \dots \cup \Gamma_{\pm\lambda_l}^n$, we mean the graph with vertex set X_n and where $\{\alpha, \beta\}$ is an edge if and only if $(\alpha, \beta) \in \Delta_{\pm\lambda_1}^n \cup \dots \cup \Delta_{\pm\lambda_l}^n$.

Conjecture 4.3.41. *Let $q = p^r$ be a prime power with $r \geq 2$. There exists a primitive element $\lambda \in \mathbb{F}_q$ such that $\Gamma_{\pm\lambda}^n \cup \Gamma_{\pm\lambda^p}^n \cup \dots \Gamma_{\pm\lambda^{p^{r-1}}}^n$ is an orbital graph of $(\text{Aut}(\Omega_3(q)), X_n)$ of diameter 2.*

4.4 $H \cap S \cong \text{PGL}_2(q^{1/2})$

In this section we analyse the diameters of the orbital graphs of the action of G on cosets of maximal subgroups H , where $S := \text{soc}(G) \cong \text{PSL}_2(q_0^2)$ (q_0 odd) and $H \cap S \cong \text{PGL}_2(q_0)$. We begin by stating the main result of the section.

Theorem 4.4.1. *Let $q \geq 5$ be odd and suppose $q = q_0^2$, for some prime power q_0 . Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong \text{PGL}_2(q_0)$. Then we have $\text{diam}_O(G, X) \leq 2$ if and only if $q_0 \equiv 3 \pmod{4}$.*

Let (G, X) be as in Theorem 4.4.1. Computations suggest that for $q_0 \equiv 1 \pmod{4}$ almost all of the orbital graphs of (G, X) have diameter 2. To be precise, we conjecture the following.

Conjecture 4.4.2. *Let $q \geq 5$ be odd and suppose $q = q_0^2$, for some prime power q_0 . Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong \text{PGL}_2(q_0)$. If $q_0 \equiv 1 \pmod{4}$, then all orbital graphs of (G, X) have diameter 2, except one.*

Conjecture 4.4.2 has been verified for values of $q_0 \leq 53$ using a computer. In particular, the one orbital graph in Conjecture 4.4.2 that does not have diameter 2 is the graph Γ_0 from Proposition 4.4.12.

Remark 4.4.3. Note that by Table 4.1, there are two conjugacy classes in $S := \text{PSL}_2(q_0^2)$ of subgroups isomorphic to $\text{PGL}_2(q_0)$; let the representatives be X_1 and X_2 . Also let $\Omega_i := (S : X_i)$ for $i = 1, 2$. We claim that the permutation groups (S, Ω_i) are permutation isomorphic and thus when analysing the diameters of the orbital graphs, it suffices to study any one of them (see Proposition 2.1.8(3)). To see this, note that by Table 4.1, the two conjugacy classes are swapped by δ . Hence there exists $t \in \text{PGL}_2(q_0^2)$ such that $t^{-1}X_1t = X_2$. Let $\dot{t}$ be the automorphism of S which is conjugation by t . Then $\dot{t}$ swaps X_1 and X_2 . Lastly, define $f : \Omega_1 \rightarrow \Omega_2$ by $X_1g \mapsto X_2\dot{t}(g)$. One can then check that $\dot{t}$ and f define a permutation isomorphism between the required permutation groups.

In order to prove Theorem 4.4.1, we will consider $\text{PSL}_2(q_0^2)$ as a subgroup of the 4-dimensional orthogonal group $O_4^-(q_0)$. Let V be a 4-dimensional vector space over $\mathbb{F}_{q_0}$ and let Q be a non-degenerate quadratic form on V with $\text{sgn}(Q) = -$. The group $O(V) \cong O_4^-(q_0)$ stabilises the quadratic form. Also $\text{SO}(V) \cong \text{SO}_4^-(q_0)$ and $\Omega(V) \cong \Omega_4^-(q_0)$. Now by Proposition 4.1.2, we have $\text{PSL}_2(q_0^2) \cong \Omega_4^-(q_0)$. Under this isomorphism the maximal subgroups $\text{PGL}_2(q_0)$ becomes the stabilisers of certain 1-dimensional subspaces of V .

We now describe an automorphism of $\Omega_4^-(q_0)$. By Proposition 2.5.12 in [14], V has a basis $\{v_1, v_2, v_3, v_4\}$ such that $(v_1, v_1) = \eta$, $(v_i, v_i) = 1$ for $i = 2, 3, 4$, and $(v_i, v_j) = 0$ for $i \neq j$, where η is a generator of $\mathbb{F}_{q_0}^*$. For the remainder of this section, we will refer to this basis as *the* orthogonal basis.

Definition 4.4.4. Let V be as above, where q_0 is a power of the odd prime p , and let $\{v_1, v_2, v_3, v_4\}$ be the orthogonal basis. We define ϕ to be the map $V \rightarrow V$, given by $av_1 + bv_2 + cv_3 + dv_4 \mapsto a^p\eta^{\frac{p-1}{2}}v_1 + b^pv_2 + c^pv_3 + d^pv_4$, for $a, b, c, d \in \mathbb{F}_{q_0}$, and we define $\dot{\phi}$ to be the map $O_4^-(q_0) \rightarrow O_4^-(q_0)$ given by $g \mapsto \phi^{-1}g\phi$.

Remark 4.4.5. Let $\{v_1, v_2, v_3, v_4\}$ be the orthogonal basis. For $u, v \in V$ write $u = a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4$ and $v = b_1v_1 + b_2v_2 + b_3v_3 + b_4v_4$, where $a_i, b_i \in \mathbb{F}_{q_0}$. Then

$$(u^\phi, v^\phi) = (a_1b_1\eta)^p + \sum_{i=2}^4 (a_ib_i)^p = \left(a_1b_1\eta + \sum_{i=2}^4 a_ib_i \right)^p = (u, v)^p.$$

Using this, it is straightforward to see that if $g \in O_4^-(q_0)$, then $\phi^{-1}g\phi$ preserves the form, and thus $\dot{\phi}(g) \in O_4^-(q_0)$. One can also easily check that $\dot{\phi}$ is a bijective homomorphism, i.e. an automorphism of $O_4^-(q_0)$.

Lemma 4.4.6. *The map $\dot{\phi}$ is an automorphism of $\Omega_4^-(q_0)$.*

Proof. By Remark 4.4.5, it suffices to show that $\dot{\phi}(\Omega_4^-(q_0)) = \Omega_4^-(q_0)$. Now, it is straightforward to check that if $\det(g) = 1$, then $\det(\phi^{-1}g\phi) = 1$, and thus $\dot{\phi}$ is an automorphism of $\text{SO}_4^-(q_0)$. Further, it is an easily proved fact that the commutator subgroup H of a group G satisfies $f(H) \leq H$ for all $f \in \text{Aut}(G)$. Since $\Omega_4^-(q_0)$ is the commutator subgroup of $\text{SO}_4^-(q_0)$, this implies that $\dot{\phi}(\Omega_4^-(q_0)) \leq \Omega_4^-(q_0)$ and the equality follows since we also have $\dot{\phi}^{-1}(\Omega_4^-(q_0)) \leq \Omega_4^-(q_0)$. $\square$

Remark 4.4.7. Note that the information on maximal subgroups of almost simple groups with socle $\text{PSL}_2(q_0^2)$ in Table 4.1, can be translated to information on maximal subgroups of almost simple groups with socle $\Omega_4^-(q_0)$ with ϕ as in Definition 4.4.4 (see Table 8.17 in [3] for the maximal subgroups of the latter).

Let X denote the set of all 1-dimensional subspaces of V . For the remainder of this section, we shall use X_s to denote the set of elements $\langle v \rangle \in X$ with $Q(v)$ a square. Note that if $\langle v \rangle$ is in X_s , then without loss of generality we may assume that $Q(v) = 1$, i.e. $(v, v) = 2$. The group $\Omega_4^-(q_0)$ acts naturally on X_s .

Proposition 4.4.8. *Let $S := \Omega_4^-(q_0)$. Then S acts transitively on X_s . Moreover, for $\alpha \in X_s$, we have $S_\alpha \cong \text{SO}_3(q_0)$.*

Proof. Firstly, we prove that S acts transitively on X_s . Let $\alpha, \beta \in X_s$ and write $\alpha := \langle v \rangle$ and $\beta := \langle w \rangle$. Then without loss of generality, we may assume that $(v, v) = (w, w)$ and so the map $i : \alpha \rightarrow \beta$, which maps $\lambda v \mapsto \lambda w$ is an isometry. Hence by Witt's Lemma there exists $g \in O_4^-(q_0)$ such that $v^g = w$. Now since every element of $O_4^-(q_0)$ has determinant ± 1 , we have that either $g \in \text{SO}_4^-(q_0)$ or $-g \in \text{SO}_4^-(q_0)$. So there exists $h \in \text{SO}_4^-(q_0)$ such that $\alpha^h = \beta$. Now, by (2.5.12) in [14], we have

$$\text{SO}_4^-(q_0) = S\langle r_x r_y \rangle, \quad (4.16)$$

where r_x and r_y are reflections in vectors $x, y \in V$ with (x, x) a square and (y, y) a non-square. Pick $x, y \in \alpha^\perp$, with (x, x) a square and (y, y) a non-square. By (4.16) there exists $h' \in S$ such that $h = h' r_x r_y$. Now $\alpha^{r_x r_y} = \alpha$ and hence $\alpha^{h'} = \beta$. This proves the transitivity of S .

Now pick a basis $\{e, f, u, v\}$ of V satisfying $Q(e) = Q(f) = (e, v) = (e, u) = (f, v) = (f, u) = (u, v) = 0$, $(e, f) = 1$, $Q(v) = 1$ and $Q(u) = -\gamma$, where $\gamma \in \mathbb{F}_q$ is a non-square (see Remark 4.4.9 for a justification for why such a basis exists). Since $\langle v \rangle \in X_s$, it suffices to show that $S_{\langle v \rangle} \cong \text{SO}_3(q_0)$. Since $\langle v \rangle$ is non-degenerate, we have $V = \langle v \rangle^\perp \perp \langle v \rangle$. Now $S_{\langle v \rangle}$ contains the subgroup $K := \langle H, r_{e+f} r_v \rangle$, where

$$H := \left\{ \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} : A \in \Omega_3(q_0) \right\},$$

and H is a normal subgroup of K . Note that $r_{e+f}r_v = \begin{pmatrix} B & 0 \\ 0 & -1 \end{pmatrix}$, where

$$B := \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and thus $r_{e+f}r_v \notin H$. Now $|K/H| = 2$ and since every element of K has determinant 1, we have $K \cong \text{SO}_3(q_0)$. Finally, note that $O_4^-(q_0)_{\langle v \rangle} \cong O_3(q_0) \times \langle -1 \rangle$ which implies $|S_{\langle v \rangle}| = \frac{1}{2}|O_3(q_0)| = |\text{SO}_3(q_0)|$ and thus $S_{\langle v \rangle} = K \cong \text{SO}_3(q_0)$. $\square$

Remark 4.4.9. Let (V, Q) be a quadratic space with bilinear form $(,)$ and basis $\beta := \{v_1, \dots, v_n\}$. Then $D(Q)$ is defined to be the determinant of the matrix $\mathbf{f}_\beta$, where $(\mathbf{f}_\beta)_{ij} := (v_i, v_j)$. For a subspace $W \subseteq V$, we define $D(W) := D(Q_W)$, where Q_W is the restriction of Q to W . Note that the value of $D(Q)$ depends on the basis $\{v_1, \dots, v_n\}$ but only up to multiplication by a square, and hence for different bases, $D(Q)$ will either always be a square or always be a non-square.

We claim that if V is a 4-dimensional vector space over $\mathbb{F}_q$ with basis $\{e, f, u, v\}$ and we define a quadratic form $Q : V \times V \rightarrow \mathbb{F}_q$ by $Q(e) = Q(f) = (e, v) = (e, u) = (f, v) = (f, u) = (u, v) = 0$, $(e, f) = 1$, $Q(v) = 1$ and $Q(u) = -\gamma$, then $\text{sgn}(Q) = -$. To see this, let $W := \langle e, f \rangle$ and observe that $V = W \perp W^\perp$. Now W contains a totally singular subspace of dimension 1 and $W^\perp$ doesn't, and so $\text{sgn}(W) = +$ and $\text{sgn}(W^\perp) = -$ (see Proposition 2.5.4(i) in [14]). Thus precisely one of $D(W)$ or $D(W^\perp)$ is a square (this follows from Proposition 2.5.10 in [14]). Since $D(Q) = D(W)D(W^\perp)$ (see Proposition 2.5.11(i) in [14]), we have that $D(Q)$ is a non-square. Now if $\text{sgn}(Q) = +$, then Proposition 2.5.10(i) in [14] implies $D(Q)$ is a square. Thus $D(Q)$ is a non-square implies $\text{sgn}(Q) = -$, as required.

Let $G := \langle \Omega_4^-(q_0), \dot{\Gamma} \rangle$ be an almost simple group with $\text{soc}(G) \cong \Omega_4^-(q_0)$ and $\dot{\Gamma} \leq \langle \dot{\phi} \rangle$. We would like to define an action of G on the set X_s ; the group $\Omega_4^-(q_0)$ acts naturally on this set, and for $v \in V$ we define $\langle v \rangle^{\dot{\phi}} := \langle v^{\dot{\phi}} \rangle$ (one can easily check that $\langle v^{\dot{\phi}} \rangle \in X_s$).

Corollary 4.4.10. *Let $G := \langle S, \dot{\Gamma} \rangle$ be an almost simple group with $S := \text{soc}(G) \cong \Omega_4^-(q_0)$, where q_0 is an odd prime power and $\dot{\Gamma} \leq \langle \dot{\phi} \rangle$. Then for $\alpha \in X_s$, we have $G_\alpha = S_\alpha \cdot \ddot{\Gamma}$ and G_α is a maximal subgroup of G .*

Proof. By Theorem 4.1.11 and Proposition 4.4.8, we have that S_α is a maximal subgroup of S , and thus G_α is a maximal subgroup of G . Also by Proposition 4.4.8, S acts transitively on X_s , and thus so does G . The rest of the proof is as in the proof of Corollary 4.3.13. $\square$

By Corollary 4.4.10, in order to analyse the primitive actions of G with $S := \text{soc}(G) \cong \text{PSL}_2(q_0^2)$ on the cosets of H where $H \cap S \cong \text{PGL}_2(q_0)$, it suffices to assume $\text{soc}(G) = \Omega_4^-(q_0)$ and analyse the natural action of G on X_s . To analyse the latter action, we will begin by analysing the particular case where $G = \Omega_4^-(q_0)$. We begin by determining the orbitals of this action.

Proposition 4.4.11. *Let $S := \Omega_4^-(q_0)$. The non-diagonal orbitals of (S, X_s) are*

$$\Delta_{\pm\lambda} := \{(\langle v \rangle, \langle w \rangle) \in X_s \times X_s : (v, v) = (w, w) = 2, (v, w) = \pm 2\lambda\},$$

where $\lambda \in \mathbb{F}_{q_0}$.

Proof. Let $\{e, f, u, v\}$ be the basis in Proposition 4.4.8. Then, we have $(\langle x \rangle, \langle y \rangle) \in \Delta_{\pm\lambda}$, where $x := v$ and $y := (1 - \lambda)e + (1 + \lambda)f + \lambda v$. Hence the sets $\Delta_{\pm\lambda}$ are non-empty. Further, it is straightforward to check that the sets $\Delta_{\pm\lambda}$ are disjoint and that their union (together with the diagonal orbital) is $X_s \times X_s$. It is also clear that if $(\langle v_1 \rangle, \langle w_1 \rangle)$ and $(\langle v_2 \rangle, \langle w_2 \rangle)$ are in the same orbital (with $(v_1, v_1) = (v_2, v_2)$ and $(w_1, w_1) = (w_2, w_2)$)

then $(v_1, w_1) = \pm(v_2, w_2)$. It remains to show that S is transitive on $\Delta_{\pm\lambda}$. Let $\alpha, \beta \in \Delta_{\pm\lambda}$ and write $\alpha = (\langle v \rangle, \langle w \rangle)$ and $\beta = (\langle v' \rangle, \langle w' \rangle)$. As in the proof of Proposition 4.3.14, we can show that there exists $h \in \text{SO}_4^-(q_0)$ such that $\alpha^h = \beta$. Now by Proposition 2.5.13(i) in [14], we have $\text{SO}_4^-(q_0) \cong S \times \langle -I_4 \rangle$, and therefore either $h \in S$ or $-h \in S$. To complete the proof it remains to note that $\alpha^{\pm h} = \beta$. $\square$

Note that since $(,)$ is symmetric, the orbitals in Proposition 4.4.11 are self-paired. We denote by $\Gamma_{\pm\lambda}$ the orbital graph corresponding to the orbital $\Delta_{\pm\lambda}$ from Proposition 4.4.11. We now prove two results concerning the diameters of these orbital graphs. Note that the condition $q = q_0^2 \geq 5$ is needed to ensure that the graphs in question are connected.

Proposition 4.4.12. *Let $q = q_0^2 \geq 5$. If $q_0 \equiv 1 \pmod{4}$, then $\text{diam}(\Gamma_0) \geq 3$.*

Proof of Proposition 4.4.12. Let $\{e, f, u, v\}$ be the basis defined in Proposition 4.4.8. Define $x := e + f$ and $y := 2f + v$. Then $Q(x) = Q(y) = 1$ and $d(\langle x \rangle, \langle y \rangle) \geq 2$. Now $d(\langle x \rangle, \langle y \rangle) = 2$ if and only if there exists $z = ae + bf + cu + dv$ with $a, b, c, d \in \mathbb{F}_{q_0}$, such that

$$ab - c^2\gamma + d^2 = 1 \tag{4.17}$$

$$a + b = 0 \tag{4.18}$$

$$a + d = 0. \tag{4.19}$$

Rearranging (4.18) and (4.19) for b and d respectively, and substituting these into (4.17), we obtain $c^2\gamma + 1 = 0$ which is a contradiction since -1 is square in $\mathbb{F}_{q_0}$. Hence $d(\langle x \rangle, \langle y \rangle) \geq 3$ from which the result follows. $\square$

Proposition 4.4.13. *Let $q = q_0^2 \geq 5$. If $q_0 \equiv 3 \pmod{4}$, then $\text{diam}(\Gamma_{\pm\lambda}) = 2$, for all $\lambda \in \mathbb{F}_q$.*

Proof. Let $\{e, f, u, v\}$ be the basis defined in Proposition 4.4.8. Let $\langle x \rangle$ and $\langle y \rangle$ be elements of X_s with $(x, y) = 2\mu$ for some $\mu \in \mathbb{F}_q$, and let

$d := d(\langle x \rangle, \langle y \rangle)$. Without loss of generality, we may suppose that $x = hu$ and $y = (1 - \mu)e + (1 + \mu)f - (\mu/h\gamma)u$, where $h^2 := -1/\gamma$. Suppose $\mu \neq \pm\lambda$, i.e. $d \neq 1$. We will show that $d = 2$. Firstly suppose that $\mu \neq \pm 1$. Then $d = 2$ if and only if there exists $z = ae + bf + cu + dv$ such that

$$ab - c^2\gamma + d^2 = 1 \quad (4.20)$$

$$-2hc\gamma = \pm 2\lambda \quad (4.21)$$

$$a(1 + \mu) + b(1 - \mu) + (2\mu c)/h = \pm 2\lambda. \quad (4.22)$$

Now (4.21) implies $c = \pm\lambda/(h\gamma)$ and substituting this into (4.22) implies

$$b = \frac{\pm 2\lambda \pm 2\mu\lambda - a(1 + \mu)}{1 - \mu}.$$

Further, substituting the expressions obtained for b and c into (4.20) and rearranging, we obtain the following quadratic equation in a :

$$(1 + \mu)a^2 \pm 2\lambda(\mu \pm 1)a + (\lambda^2 + d^2 - 1)(\mu - 1) = 0.$$

The discriminant of this quadratic equation (choosing $+$ for the second $\pm$) is

$$B(d) := (1 - \mu^2)d^2 - (1 + \mu)(1 - \mu - 2\lambda^2).$$

In order to prove the existence of z , it suffices to show that for each λ and each $\mu \neq \pm 1, \pm\lambda$, there exists d such that $B(d)$ is a square. This is equivalent to showing that for each λ and $\mu \neq \pm 1, \pm\lambda$ there exist d, y such that

$$(1 - \mu^2)d^2 - y^2 = (1 + \mu)(1 - \mu - 2\lambda^2). \quad (4.23)$$

We show the latter by considering the following two cases. Suppose first that $1 - \mu^2$ is a square. Since every element of a finite field with odd characteristic can be expressed as the difference of two squares (see Lemma A.9 in

Appendix A), there exist $\alpha, \beta \in \mathbb{F}_{q_0}$ such that

$$\alpha^2 - \beta^2 = (1 + \mu)(1 - \mu - 2\lambda^2).$$

Pick d and y such that $d^2 = \alpha^2/(1 - \mu^2)$ and $y = \beta$. Then (4.23) holds. Now suppose that $1 - \mu^2$ is a non-square and $\mu \neq 1 - 2\lambda^2$. Since $q = q_0^2 \geq 9$, every non-zero element of $\mathbb{F}_{q_0}$ can be expressed as the sum of two non-squares (see Lemma A.12 in Appendix A), and hence there exist non-squares $\alpha, \beta \in \mathbb{F}_{q_0}$ such that

$$\alpha + \beta = (1 + \mu)(1 - \mu - 2\lambda^2).$$

Pick d and y such that $d^2 = \alpha/(1 - \mu^2)$ and $y^2 = -\beta$ (note that -1 is non-square since $q_0 \equiv 3 \pmod{4}$). Then (4.23) holds. If $\mu = 1 - 2\lambda^2$, then (4.23) holds with $y = d = 0$. In conclusion, z exists for $\mu = \pm 1$. If $\mu = 1$, then let $z := -2\lambda e + (\lambda/2)f - (\lambda/(h\gamma))u + v$, and if $\mu = -1$, then let $z := -(\lambda/2)e + (2\lambda)f - (\lambda/(h\gamma))u + v$. Then $\langle x \rangle - \langle z \rangle - \langle y \rangle$ is a path of length 2 and hence $d(\langle x \rangle, \langle y \rangle) = 2$. The result follows. $\square$

To analyse the orbital graphs of (G, X_s) , where $G := \langle S, \dot{\Gamma} \rangle$ is an almost simple group with $S := \text{soc}(G) \cong \Omega_4^-(q_0)$ and $\dot{\Gamma} \leq \langle \dot{\phi} \rangle$, we will need to determine the action of $\dot{\phi}$ on the orbitals $\Delta_{\pm\lambda}$ of $(\Omega_4^-(q_0), X_s)$. The action of $\dot{\phi}$ on $\Delta_{\pm\lambda}$ will be denoted by $(\Delta_{\pm\lambda})^{\dot{\phi}}$.

Proposition 4.4.14. *Let $\Delta_{\pm\lambda}$ be an orbital of $(\Omega_4^-(q_0), X_s)$, where q_0 is a power of the prime p . Then $(\Delta_{\pm\lambda})^{\dot{\phi}} = \Delta_{\pm\lambda^p}$.*

Proof. Let $\{v_1, v_2, v_3, v_4\}$ be the orthogonal basis. Recall from Remark 4.4.5 that for $u, v \in V$, we have

$$(u^\phi, v^\phi) = (u, v)^p. \tag{4.24}$$

Suppose $(\langle x \rangle, \langle y \rangle) \in \Delta_{\pm\lambda^p}$, where $(x, x) = (y, y) = 2$ and $(x, y) = \pm 2\lambda^p$.

Write

$$x = x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4, \quad y = y_1v_1 + y_2v_2 + y_3v_3 + y_4v_4,$$

for some $x_i, y_i \in \mathbb{F}_q$. Now, define

$$x' := cx_1^{1/p}v_1 + x_2^{1/p}v_2 + x_3^{1/p}v_3 + x_4^{1/p}v_4, \quad y' := cy_1^{1/p}v_1 + y_2^{1/p}v_2 + y_3^{1/p}v_3 + y_4^{1/p}v_4,$$

where $c^2 = \eta^{1/p}\eta^{-1}$. Then using (4.24) one can check that $(\langle x' \rangle, \langle y' \rangle) \in \Delta_{\pm\lambda}$ and $(\langle x' \rangle, \langle y' \rangle)^\phi = (\langle x \rangle, \langle y \rangle)$. This proves that $\Delta_{\pm\lambda^p} \subseteq (\Delta_{\pm\lambda})^\phi$. For the converse, suppose $(\langle x \rangle, \langle y \rangle) \in \Delta_{\pm\lambda}$, where $(x, x) = (y, y) = 2$ and $(x, y) = \pm 2\lambda$. Then using (4.24) one can check that

$$(x^\phi, x^\phi) = (y^\phi, y^\phi) = 2, \quad (x^\phi, y^\phi) = \pm 2\lambda^p,$$

and thus $(\langle x \rangle, \langle y \rangle)^\phi \in \Delta_{\pm\lambda^p}$. This proves that $(\Delta_{\pm\lambda})^\phi \subseteq \Delta_{\pm\lambda^p}$. $\square$

Proof of Theorem 4.4.1. Let G and X be as in the statement of the theorem. By Proposition 4.1.2 and Corollary 4.4.10, we may suppose that $\text{soc}(G) = \Omega_4^-(q_0)$ and $X = X_s$. By Proposition 4.4.14, Γ_0 is an orbital graph of (G, X) . Moreover, by Proposition 4.4.12 we have $\text{diam}(\Gamma_0) \geq 3$ if $q_0 \equiv 1 \pmod{4}$. Hence $\text{diam}_O(G, X) \leq 2$ implies $q_0 \equiv 3 \pmod{4}$. Conversely, suppose $q_0 \equiv 3 \pmod{4}$ and let Γ be an orbital graph of (G, X) . Then $\text{diam}(\Gamma) \leq \max_\lambda \{\text{diam}(\Gamma_{\pm\lambda})\} = 2$, where the equality holds by Proposition 4.4.13. $\square$

4.5 $H \cap S \cong \text{PSL}_2(q^{1/t})$

In this section we analyse the diameters of the orbital graphs of the action of G on the cosets of maximal subgroups H , where $S := \text{soc}(G) \cong \text{PSL}_2(q_0^t)$ (q_0 odd) with t an odd prime, and $H \cap S \cong \text{PSL}_2(q_0)$. We begin by stating the main result of the section.

Theorem 4.5.1. *Let $q \geq 5$ be odd and suppose $q = q_0^t$, where t is an odd prime. Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong \text{PSL}_2(q_0)$.*

1. *If $\text{diam}_O(G, X) \leq 2$, then $t = 3$.*
2. *Let $G \cong \text{PSL}_2(q)$. The following hold:*
 - (a) $\text{diam}_O(G, X) > 2$;
 - (b) (G, X) has no orbital graphs of diameter 2;
 - (c) *if there exist orbital graphs of diameter 3, then $t = 3$.*

In order to prove part 1 of Theorem 4.5.1 we will need the following result.

Lemma 4.5.2. *Let (G, X) be as in the statement of Theorem 4.5.1, with $q = p^r$ for some odd prime p . If (G, X) has an orbital graph Γ of diameter d , then*

$$2.99 - \frac{3d+3}{t} < d \log_q(2r) + \log_q \left(\frac{144}{143} \right).$$

Proof. By Lemma 2.2.1 we have

$$\begin{aligned} |G : H| &\leq 1 + v + v(v-1) + v(v-1)^2 + \cdots + v(v-1)^{d-1} \\ &< 1 + v + v^2 + v^3 + \cdots + v^d, \end{aligned} \tag{4.25}$$

where $v := 2|H|$. Define $A := \text{Aut}(S)$ and define J to be the maximal subgroup of A such that $J/(H \cap S) \cong \text{Out}(S)$. Since $|G : H| = |A : J|$ and $|H| \leq |J|$, using (4.25) we obtain

$$|A| < \left(\frac{2|J|^{d+1} - 1}{2|J| - 1} \right) |J| < \frac{|J|}{2|J| - 1} (2|J|)^{d+1}.$$

This implies

$$q(q^2 - 1)r < (2q_0^3 r)^{d+1} \frac{1}{2 - \frac{1}{|J|}}.$$

Note that since q is odd, we have $q_0 \geq 3$. Also, since t is an odd prime dividing r , we have $r \geq 3$. These imply $|J| = q_0(q_0^2 - 1)r \geq 72$, and using this in the above we obtain

$$q(q^2 - 1) < (2r)^d q_0^{3d+3} \frac{144}{143}.$$

Now $q \geq 27$ which implies $q^{2.99} < q(q^2 - 1)$. Using this in the above we obtain

$$q^{2.99} < (2r)^d q^{\frac{3d+3}{t}} \frac{144}{143}.$$

Rearranging the above, we obtain the result, i.e.

$$2.99 - \frac{3d+3}{t} < d \log_q(2r) + \log_q \left(\frac{144}{143} \right).$$

□

We now prove Theorem 4.5.1.

Proof of Theorem 4.5.1(1). Suppose $\text{diam}_O(G, X) \leq 2$. Then (G, X) has an orbital graph of diameter $d \leq 2$. Therefore using Lemma 4.5.2, we have

$$2.99 - \frac{9}{t} < 2 \log_q(2r) + \log_q \left(\frac{144}{143} \right). \quad (4.26)$$

Now $\log_q \left(\frac{144}{143} \right)$ is a decreasing function of q . In particular, since $q \geq 27$, we have $\log_q \left(\frac{144}{143} \right) \leq 0.0021$. Similarly, since $\log_q(2r) = \log_{p^r}(2r)$ is a decreasing function of p , we have $\log_{p^r}(2r) \leq \log_{3^r}(2r)$, where $q = p^r$ and p is a prime. Furthermore, $\log_{3^r}(2r)$ is also a decreasing function of r , hence since $r \geq 3$, we have $\log_{p^r}(2r) \leq 0.5437$. Now rearranging (4.26) for t using these upper bounds, we conclude that $t = 3$. □

Proof of Theorem 4.5.1(2). Suppose $\text{diam}_O(G, X) \leq 2$. By Theorem 4.5.1(1), we must have $t = 3$. Then by Lemma 2.2.1, we have

$$|G : H| \leq 1 + 2|H| + 2|H|(2|H| - 1) = 1 + 4|H|^2.$$

Now substituting $|G| = \frac{q(q^2-1)}{2}$ and $|H| = \frac{q^{1/3}(q^{2/3}-1)}{2}$ into the above and simplifying, we obtain $f(q) \geq 0$, where

$$f(q) := q - q^{1/3} - 3q^{7/3} + 3q^{5/3}.$$

However it is not hard to show that $f(q) < 0$ for all $q \geq 5$ which is a contradiction. The same contradiction arises if we suppose that (G, X) has an orbital graph of diameter 2.

Now suppose (G, X) has an orbital graph of diameter 3. Then by using Lemma 4.5.2 with $d = 3$, we have

$$2.99 - \frac{12}{t} < 3 \log_q(2r) + \log_q \left(\frac{144}{143} \right).$$

As in the proof of Theorem 4.5.1(1), we have $\log_q \left(\frac{144}{143} \right) \leq 0.0021$, and if $r \geq 5$, then $\log_q(2r) \leq \log_{3r}(2r) \leq 0.4192$. Using these in the above inequality and rearranging for t we obtain $t = 3$ or $t = 5$. If $r \leq 4$, then $r = t = 3$. So in either case we have $t = 3$ or $t = 5$. We claim that $t = 5$ cannot occur. Suppose there exist orbital graphs of diameter 3 for $t = 5$. Then using (4.25) we obtain $|G| < 16|H|^5$, i.e.

$$q(q^2 - 1) < q^{5/t}(q^{2/t} - 1)^5 = q(q^{2/5} - 1)^5.$$

Simplifying the above we obtain $f(q) > 0$, where

$$f(q) := 2q^{6/5} + q^{2/5} - 2q^{4/5} - q^{8/5}.$$

However it is not hard to show that $f(q) < 0$ for all $q \geq 5$, a contradiction. $\square$

4.6 $H \cap S \cong A_4, A_5, S_4$

In this section we analyse the diameters of the orbital graphs of the action of G on the cosets of maximal subgroups H , where $S := \text{soc}(G) \cong \text{PSL}_2(q)$ (q odd) and $H \cap S \cong A_4, A_5$ or S_4 . We begin by stating the main theorem of the section. Recall that $\dot{\delta}$ and $\dot{\phi}$ are the automorphisms of $\text{PSL}_2(q)$ from Section 4.1 and that $\ddot{\delta}$ and $\ddot{\phi}$ are their images in $\text{Out}(\text{PSL}_2(q))$.

Theorem 4.6.1. *Let $q \geq 5$ be odd. Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong A_4, A_5$ or S_4 .*

1. *Let $c \geq 1$. If $\text{diam}_O(G, X) \leq c$, then $q < \epsilon m^{\frac{10c}{29}}$, where ϵ and m are as in Table 4.7.*
2. *We have $\text{diam}_O(G, X) \leq 2$ if and only if G and H are as in Table 4.8.*
3. *(G, X) has orbital graphs of diameter 2 if and only if G and H are as in Table 4.9.*

G	H	ϵ	m
$\text{PSL}_2(q)$	A_4	3.083	23
$\text{PSL}_2(q) \cdot \langle \ddot{\delta} \rangle$	$A_4 \cdot \langle \ddot{\delta} \rangle$	3.037	47
$\text{PSL}_2(q)$	A_5	5.242	119
$\text{PSL}_2(q) \cdot \langle \ddot{\phi} \rangle$	$A_5 \cdot \langle \ddot{\phi} \rangle$	5.227	239
$\text{PSL}_2(q)$	S_4	3.856	47

Table 4.7: $\text{diam}_O(G, X) \leq c \Rightarrow q < \epsilon m^{\frac{10c}{29}}$, where $X := (G : H)$

G	H	Notes
$\text{PSL}_2(5)$	A_4	
$\text{PSL}_2(5).\langle\ddot{\delta}\rangle$	$A_4.\langle\ddot{\delta}\rangle$	
$\text{PSL}_2(q)$	A_5	$q \in \{9, 11\}$
$\text{PSL}_2(9).\langle\ddot{\phi}\rangle$	$A_5.\langle\ddot{\phi}\rangle$	
$\text{PSL}_2(7)$	S_4	

Table 4.8: Pairs (G, X) with $\text{diam}_O(G, X) \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$

G	H	Notes
$\text{PSL}_2(13)$	A_4	
$\text{PSL}_2(q).\langle\ddot{\delta}\rangle$	$A_4.\langle\ddot{\delta}\rangle$	$q \in \{11, 13\}$
$\text{PSL}_2(q)$	A_5	$q \in \{19, 29, 31, 41, 49, 61\}$
$\text{PSL}_2(49).\langle\ddot{\phi}\rangle$	$A_5.\langle\ddot{\phi}\rangle$	
$\text{PSL}_2(q)$	S_4	$q \in \{17, 23\}$

Table 4.9: Orbital graphs of diameter 2 for (G, X) , where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$

Remark 4.6.2.

1. Let G and H be as in the statement of Theorem 4.6.1. All such pairs (G, H) can be deduced from Table 4.1 and are given explicitly by the first two columns of Table 4.7. These columns are repeated in Tables 4.10 and 4.11.
2. Note that $\text{PSL}_2(5) \cong A_5$ (see [24, p. 51]) and thus the cases with $q = 5$ in Table 4.8 are equivalent to the actions of A_5 and S_5 on 1-subsets of $\{1, \dots, 5\}$. Similarly, since $\text{PSL}_2(9) \cong A_6$ (see [24, p. 52]), the cases with $q = 9$ in Table 4.8 are equivalent to the actions of A_6 and S_6 on 1-subsets of $\{1, \dots, 6\}$. The primitive actions of A_n and S_n have already been studied in Chapter 3.

Proof of Theorem 4.6.1(1). Let (G, H) be a pair from the first two columns of Table 4.7. Using the fact that $|\text{PSL}_2(q)| = \frac{q(q^2-1)}{2}$, for $H \cap S \cong A_4, A_5$ or S_4 , respectively we have

$$|G : H| = \frac{q(q^2-1)}{24}, \frac{q(q^2-1)}{120}, \frac{q(q^2-1)}{48}. \quad (4.27)$$

Also, for $q \geq 5$ we have

$$q^{29/10} < q(q^2-1). \quad (4.28)$$

Now if $\text{diam}_O(G, X) \leq c$, then (G, X) has an orbital graph of diameter $d \leq c$. We then obtain the result by using (2.3) from Lemma 2.2.1, (4.27) and (4.28) for the pair (G, H) , and rearranging for q . $\square$

We would now like to prove Theorem 4.6.1(2) and (3). To do this, one could start by using Theorem 4.6.1(1) with $c = 2$. However, doing so may produce values of q which may not be possible using (2.2) from Lemma 2.2.1. Thus we use the upper bound in (2.2) directly to obtain the following result.

Proposition 4.6.3. *Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong A_4, A_5$ or S_4 . If (G, X) has an orbital graph of diameter $c \leq 2$, then G and H are as in Table 4.10.*

G	H	Possible values of q
$\text{PSL}_2(q)$	A_4	$q \leq 24, q = p \equiv \pm 3, 5, \pm 13 \pmod{40}$
$\text{PSL}_2(q). \langle \ddot{\delta} \rangle$	$A_4. \langle \ddot{\delta} \rangle$	$q \leq 38, q = p \equiv \pm 3, 5, \pm 13 \pmod{40}$
$\text{PSL}_2(q). \langle \ddot{\delta} \rangle$	$A_4. \langle \ddot{\delta} \rangle$	$q \leq 38, q = p \equiv \pm 11, \pm 19 \pmod{40}$
$\text{PSL}_2(q)$	A_5	$q \leq 120, q = p \equiv \pm 1 \pmod{10}$
$\text{PSL}_2(q)$	A_5	$q \leq 120, q = p^2, p \equiv \pm 3 \pmod{10}$
$\text{PSL}_2(q). \langle \ddot{\phi} \rangle$	$A_5. \langle \ddot{\phi} \rangle$	$q \leq 190, q = p^2, p \equiv \pm 3 \pmod{10}$
$\text{PSL}_2(q)$	S_4	$q \leq 48, q = p \equiv \pm 1 \pmod{8}$

Table 4.10: Possible pairs (G, X) with orbital graph of diameter $c \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$

Proof. Let (G, H) be a pair from the first two columns of Table 4.10. The third column contains the congruences of q for which each pair occurs (as described in Table 4.1). The upper bounds for q can then be obtained by using (2.2) from Lemma 2.2.1 with $d := c \leq 2$. $\square$

Proposition 4.6.4. *Let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where $H \cap S \cong A_4, A_5$ or S_4 . If $\text{diam}_O(G, X) \leq 2$, then G and H are as in Table 4.11.*

G	H	Possible values of q
$\text{PSL}_2(q)$	A_4	5
$\text{PSL}_2(q) \cdot \langle \ddot{\delta} \rangle$	$A_4 \cdot \langle \ddot{\delta} \rangle$	5, 11
$\text{PSL}_2(q)$	A_5	9, 11, 19, 29
$\text{PSL}_2(q) \cdot \langle \ddot{\phi} \rangle$	$A_5 \cdot \langle \ddot{\phi} \rangle$	9
$\text{PSL}_2(q)$	S_4	7

Table 4.11: Possible pairs (G, X) with $\text{diam}_O(G, X) \leq 2$, where $S := \text{soc}(G) \cong \text{PSL}_2(q)$, $X := (G : H)$ and $H \cap S \cong A_4, A_5, S_4$

Proof. Let (G, H) be a pair from the first two columns of Table 4.11. Suppose $\text{diam}_O(G, X) \leq 2$. Then (G, X) has an orbital graph of diameter $c \leq 2$, hence by Proposition 4.6.3, the value of q must be in Table 4.10; let $L_{[q_{\text{old}}]}$ denote the list consisting of these values. We use the computer program $C_{\text{LOW}}^{G,H}(2, L_{[q_{\text{old}}]})$ (detailed in Section 5.7 in Chapter 5) to compute the largest subgroup $Y \leq H$ satisfying the assumption of Proposition 2.2.2 and output a new list $L_{[q_{\text{new}}]}$ which consists of only those values in $L_{[q_{\text{old}}]}$ for which the lower bound for the diameter in Proposition 2.2.2 is strictly less than 2. Thus the permutation group corresponding to each discarded value of q has an orbital graph of diameter at least 3 and hence these discarded values cannot occur. The values of q which remain in $L_{[q_{\text{new}}]}$ are precisely the ones in Table 4.11. $\square$

Proof of Theorem 4.6.1(2) and (3). Let G and H be as in the statement of the theorem. If $\text{diam}_O(G, X) \leq 2$, then by Proposition 4.6.4, the value of q must be in Table 4.11. For each such value of q , we then use the computer program $C_{\text{DIAM}}^{G,H}(q)$ (detailed in Section 5.8 in Chapter 5) to output the diameters of the orbital graphs of (G, X) and verify that the only values of q for which $\text{diam}_O(G, X) \leq 2$ are the ones in Table 4.8. This proves part 2. Similarly, if (G, X) has an orbital graph of diameter 2 then the value of q must be in Table 4.10, and we again use $C_{\text{DIAM}}^{G,H}(q)$ to output the diameters of the orbital graphs of (G, X) and verify that the only values of q for which (G, X) has orbital graph of diameter 2 are the ones in Table 4.9. This proves part 3. $\square$

4.7 Proof of the main result

Proof of Theorem 4.2.1. Let $q \geq 17$ be odd and let (G, X) be a primitive permutation group with $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $X := (G : H)$, where H is a maximal subgroup of G , not containing S . The possibilities for $H \cap S$ are listed in Table 4.1. Suppose $\text{diam}_O(G, X) \leq 2$. If $H \cap S = P_1$, then (G, X) is 2-transitive (see Remark 4.1.12), and thus there is only one orbital graph which has diameter 1, and so $\text{diam}_O(G, X) \leq 2$ for this case. If $H \cap S \cong D_{q \mp 1}$, or $H \cap S \cong \text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 1 \pmod{4}$, or $H \cap S \cong \text{PSL}_2(q^{1/t})$ with $t \geq 4$, or $H \cap S \cong A_4, S_4, A_5$, then Theorems 4.3.1(1), 4.3.2(1), 4.4.1, 4.5.1(1) and 4.6.1(2) imply that (G, X) has an orbital graph of diameter at least 3. Hence the cases which can occur are $H \cap S = P_1$, or $H \cap S \cong \text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 3 \pmod{4}$, or $H \cap S \cong \text{PSL}_2(q^{1/3})$. The converse for $H \cap S = P_1$ has already been established, and the converse for $H \cap S \cong \text{PGL}_2(q^{1/2})$ with $q^{1/2} \equiv 3 \pmod{4}$ can be found in Theorem 4.4.1. Now suppose $G \cong \text{PSL}_2(q)$. Part 2a is a concatenation of Theorems 4.3.1(2) and 4.4.1. Part 2b is a concatenation of Theorems 4.3.2(2) and 4.5.1(2). Finally, part 2c is Theorem 4.6.1(3). $\square$

The diameters and valencies of the orbital graphs of the primitive permutation group (G, X) where $S := \text{soc}(G) \cong \text{PSL}_2(q)$ with $X := (G : H)$ and $S \not\leq H <_{\max} G$, when $q \leq 13$ is odd, can be found in Table 4.2. The first three columns of the table can be obtained from Table 4.1. For each odd prime power $q \leq 13$, we use the computer program $C_{\text{DIAM}}^{\text{PSL}_2}(q)$ (detailed in Section 5.9 in Chapter 5) to compute the diameters of the orbital graphs of (G, X) . The output includes the orders of G and H , however in certain cases these have not been enough to identify G and H with the groups G and H in Table 4.2 (due to their being multiple groups of the same order). This happens in two cases; one where it needs to be distinguished whether $H \cap S$ is a dihedral group or an alternating group, and the other where $H \cap S$ is dihedral but it needs to be decided whether or not $G = \text{PGL}_2(q)$. In the former case we use the computer program $C_{\text{D}\pm}^{\text{PSL}_2}(q)$ to output the diameters of all the orbital graphs of (G, X) where $H \cap S \cong D_{q\pm 1}$. We then compare this output with the output from the two cases which need to be distinguished and identify the output which corresponds to the case with $H \cap S$ being alternating. In the latter case we use the computer program $C_{\text{DIAM}}^{\text{PGL}_2}(q)$ to output the diameters of all orbital graphs of (G, X) where $G = \text{PGL}_2(q)$. Again comparing this with the indistinguishable outputs we can identify the output which does not correspond to $G = \text{PGL}_2(q)$. The programs are detailed in Sections 5.10 and 5.11 in Chapter 5.

Chapter 5

Computations using Magma

In this chapter we detail the computer programs that have been used in Chapters 3 and 4. In particular, we present pseudocode for each program. The source code for each of the programs detailed in this chapter has been written on the computer algebra system Magma [2] which has a vast library of predefined functions to deal with permutation groups.

5.1 $C_{\text{DIAM}}^G(k, l)$, $G = S_n$

In this section we detail the computer program $C_{\text{DIAM}}^G(k, l)$ for $G = S_n$ which is used in the proof of Theorem 3.2.6(2). This program takes as inputs integers $k, l > 1$. It outputs the rank of $(S_{kl}, I^{(k,l)})$ and for each orbital of $(S_{kl}, I^{(k,l)})$ it outputs the diameter of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired.

The pseudocode for $C_{\text{DIAM}}^G(k, l)$ with $G = S_n$ can be found in Pseudocode 1. We now explain the pseudocode. Lines 1 to 19 are self-explanatory; by the end we have defined the permutation group $P = (S_{kl}, I^{(k,l)})$ (the set being acted on is enumerated automatically by numbers $1, 2 \dots$) and its sub-orbits, and have output the rank of the action. In order to compute the

diameters of all the orbital graphs we can either use two predefined functions to firstly construct the orbital graphs and then compute their diameters, or we can use an alternative approach which involves working out the diameters of the corresponding *collapsed graphs*. The first method is fairly easy to code but turns out to be inefficient when the index of $S_k \wr S_l$ in S_{kl} becomes large; the orbital graphs have too many vertices which cannot be dealt with using the current computing facilities. Therefore we adopt the alternative method which eliminates the need to construct the orbital graphs explicitly; this method still has limitations when the index becomes large, but can deal with higher values of k and l compared to the first approach. The method is as follows.

Let G be a transitive permutation group acting on a finite set Ω . Let $\Omega_1 := \{\alpha\}, \Omega_2, \dots, \Omega_r$ be the distinct orbits of G_α on Ω , with representatives $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_r$. Let E be a union of orbitals of (G, Ω) . Define an $r \times r$ matrix A_E where for $k, j \in \{1, \dots, r\}$,

$$(A_E)_{kj} := |E(\alpha_k) \cap \Omega_j|$$

and $E(\alpha_k) := \{\gamma \in \Omega : (\alpha_k, \gamma) \in E\}$. Note that A_E does not depend on the choice of the suborbit representatives and is defined with-respect to an ordering of the suborbits. Let Δ be an orbital of (G, Ω) . We define the *collapsed adjacency matrix* for the orbital graph Γ corresponding to the orbitals Δ and Δ^* to be the matrix A_E , where $E := \Delta \cup \Delta^*$. The corresponding *collapsed graph* is defined to be Γ^C , with vertex set $\{1, \dots, r\}$, and in which (k, j) is an edge if $(A_E)_{kj} > 0$. It is a fact that $\text{diam}(\Gamma) = \text{diam}(\Gamma^C)$ (see Theorem 3.2B in [19]), and thus to compute the diameters of the orbital graphs of P , it suffices to compute the diameters of the corresponding collapsed graphs. The latter can be done via the collapsed adjacency matrices which are calculated in the next part of the code. Observe that if $E := \Delta_i$ is a single orbital

corresponding to the suborbit Ω_i , then

$$(A_E)_{kj} = |E(\alpha_k) \cap \Omega_j| = |\Omega_i^{w_k} \cap \Omega_j|, \quad (5.1)$$

where w_k is the *trace* of α_k (see the next paragraph). Thus if Δ_i is self-paired then (5.1) can be used to compute the corresponding collapsed adjacency matrix. If Δ is an orbital which is not self-paired, then $A_{\Delta \cup \Delta^*} = A_\Delta + A_{\Delta^*}$ (see Proposition 2.2 in [19]).

In Lines 20 to 23, we calculate the *trace* of each suborbit representative γ , i.e. the element g of P such that $1^g = \gamma$ (we have chosen $\alpha = 1$ in the previous paragraph). The *trace* function is not predefined in Magma; see Pseudocode 2 for details of its construction. For the remainder of the code we do the following for each suborbit Δ . In Lines 25 to 32, we compute the entries of the matrix A_Δ using (5.1). During this process we make use of the function *suborb* (again this function is not predefined and is detailed in Pseudocode 3) to compute which suborbit (from an ordered list) a given element belongs to. In Lines 33 to 38, we check whether or not Δ is self-paired. It is not hard to show that Δ is self-paired if and only if there exists l such that $(A_\Delta)_{1l} * (A_\Delta)_{l1} \neq 0$. In Lines 39 to 58, we define the collapsed adjacency matrix of the orbital graph corresponding to Δ using the techniques described in the previous paragraph. In particular, if Δ is not self-paired and has suborbit representative β , then Δ^* has suborbit representative $1^{h^{-1}}$, where h is the trace of β . We use this to find the suborbit corresponding to Δ^* and calculate A_{Δ^*} in a similar way to A_Δ . Let N denote the collapsed adjacency matrix. Then the diameter of the collapsed graph and hence of the orbital graph in question, is just the least number r of times N has to be multiplied by itself before each non-diagonal entry has taken a value greater than zero at least once. The number r is what is calculated in Lines 59 to 81.

Note that Lines 11 to 81 only require a group G and maximal subgroup H to be defined, and thus we can re-use this part of the pseudocode whenever we have such a G and H to work out the diameters of all the orbital graphs

of $(G, (G : H))$. On the other hand, this piece of code also has limitations. In Line 11, Magma is only able to define the permutation group $(G, (G : H))$ if the index of H in G is not ‘too large’, and otherwise outputs an error. This gives rise to a few unsolved cases in some of the main results in Chapter 3.

Also note that in Lines 41 and 57, we calculate the valency of the orbital graph corresponding to the i^{th} suborbit; this information is not needed as an output in this particular code, however it will be needed in later codes, where we reuse this part of the code.

Pseudocode 1 $C_{\text{DIAM}}^{S_n}(k, l)$

```
1: define  $a := k$ 
2: define  $b := l$ 
3: define  $G := S_{ab}$ 
4: define  $x := a!^b b!$ 
5: define  $max$  to be the set of subgroups of  $G$  of cardinality  $x$ 
6: for  $J$  in  $max$  do
7:   if  $J \cong S_a \wr S_b$  then
8:     define  $H := J$ 
9:   end if
10: end for
11: define  $P$  to be the permutation group  $(G, (G : H))$ 
12: define  $stab$  to be the stabiliser in  $P$  of the element 1
13: define  $suborbits$  to be the list of orbits of  $stab$ 
14: define an empty list  $suborbitReps$ 
15: for  $X$  in  $suborbits$  do
16:   Include in  $suborbitReps$ , the first element of  $X$ 
17: end for
18: define  $rank$  to be the number of element in  $suborbitReps$ 
19: output  $rank$ 
20: define an empty list  $tracesOfSuborbitReps$ 
21: for  $i$  in  $[1, rank]$  do
22:   define  $tracesOfSuborbitReps[i] := trace(suborbitReps[i])$ 
23: end for
24: for  $i$  in  $[1, rank]$  do
25:   define an empty matrix  $Q$ 
26:   for  $k$  in  $[1, rank]$  do
27:     for  $\beta$  in  $suborbits[i]$  do
28:       define  $j := suborb(\beta^{tracesOfSuborbitReps[k]})$ 
29:       add 1 to  $Q_{kj}$ 
30:     end for
31:   end for
32:   define  $colAdjMat1 := Q$ 
33:   define  $selfPaired := false$ 
```

```

34:   for  $l$  in  $[1, rank]$  do
35:       if  $colAdjMat1[1][l] * colAdjMat1[1][l] \neq 0$  then
36:           set  $selfPaired := \mathbf{true}$ 
37:       end if
38:   end for
39:   if  $selfPaired = \mathbf{true}$  then
40:       define  $colAdjMat := colAdjMat1$ 
41:       define  $valency$  to be the size of  $suborbits[i]$ 
42:   end if
43:   if  $selfPaired = \mathbf{false}$  then
44:       define  $\beta$  to be the first element of  $suborbits[i]$ 
45:       define  $g := trace(\beta)^{-1}$ 
46:       define  $\gamma := 1^g$ 
47:       define  $t := suborb(\gamma)$ 
48:       define an empty matrix  $R$ 
49:       for  $k$  in  $[1, rank]$  do
50:           for  $\beta$  in  $suborbits[t]$  do
51:               define  $j := suborb(\beta^{tracesOfSuborbitReps[k]})$ 
52:               add 1 to  $R_{kj}$ 
53:           end for
54:       end for
55:       define  $colAdjMat2 := R$ 
56:       set  $colAdjMat := colAdjMat1 + colAdjMat2$ 
57:       define  $valency$  to be twice the size of  $suborbits[i]$ 
58:   end if
59:   define an empty list  $L$  consisting of  $rank$  empty lists of size  $rank$ 

```

```

60:   for  $r$  in  $[1, rank]$  do
61:       define  $N := colAdjMat^r$ 
62:       for  $k$  in  $[1, rank]$  do
63:           for  $j$  in  $[1, rank]$  do
64:               if  $N_{kj} \neq 0$  and  $k \neq j$  then
65:                   Insert 1 into the  $j$ th position of the  $k$ -th list in  $L$ 
66:               end if
67:           end for
68:       end for
69:       define  $numberOfNonzeroEntries := 0$ 
70:       for  $k$  in  $[1, rank]$  do
71:           for  $j$  in  $[1, rank]$  do
72:               if  $L[k][j] = 1$  and  $k \neq j$  then
73:                   Add 1 to  $numberOfNonzeroEntries$ 
74:               end if
75:           end for
76:       end for
77:       if  $numberOfNonzeroEntries = rank^2 - rank$  then
78:           output  $r, selfPaired$ 
79:       end if
80:   end for
81: end for

```

In Pseudocode 1, the trace of an element γ is computed through a recursive function called *trace*. The construction of this function is described in Pseudocode 2. We now explain the code. The purpose of Lines 2 to 19 is to construct two lists V and W , where W consists of each element of the set being acted on, precisely once and V contains the indexes of the generators $x_1, \dots, x_t$ of P , such that $W[\gamma]^{x_V[\gamma]} = \gamma$. In the remaining code, we define the outputs of the function, which are fairly self-explanatory given the previous discussion.

Pseudocode 2 $trace(\gamma)$

```
1: function  $trace(\gamma)$ 
2:   define an empty list  $V$ 
3:   define an empty list  $W$ 
4:   define  $orbit := \{1\}$ 
5:   define  $stillLeft := \{1\}$ 
6:   define  $X$  to be a list of generators of  $P$ 
7:   while  $stillLeft$  is non-empty do
8:     for  $\delta$  in  $stillLeft$  do
9:       for  $i$  in  $[1, |X|]$  do
10:        if  $\delta^{X[i]}$  is not in  $orbit$  then
11:          include in  $orbit$ , the element  $\delta^{X[i]}$ 
12:          define  $V[\delta^{X[i]}] := i$ 
13:          define  $W[\delta^{X[i]}] := \delta$ 
14:          include in  $stillLeft$ , the element  $\delta^{X[i]}$ 
15:        end if
16:      end for
17:      exclude from  $stillLeft$ , the element  $\delta$ 
18:    end for
19:  end while
20:  if  $\gamma = 1$  then
21:    return the identity element of  $P$ 
22:  else
23:    return  $trace(W[\gamma]) * X[V[\gamma]]$ 
24:  end if
25: end function
```

In Pseudocode 1, we use the function *suborb* to compute which suborbit (from an ordered list) a given element belongs to. The construction of this function is described in Pseudocode 3 and is fairly self-explanatory.

Pseudocode 3 $suborbit(\gamma)$

```
1: function  $suborbit(\gamma)$ 
2:   for  $i$  in  $[1, rank]$  do
3:     if  $\gamma$  is in  $suborbits[i]$  then
4:       return  $i$ 
5:     end if
6:   end for
7: end function
```

5.2 $C_{\text{DIAM}}^G(k, l)$, $G = A_n$

In this section we detail the computer program $C_{\text{DIAM}}^G(k, l)$ for $G = A_n$ which is used in the proof of Theorem 3.2.6(2). This program takes as inputs integers $k, l > 1$. It outputs the rank of $(A_{kl}, I^{(k,l)})$ and for each orbital of $(A_{kl}, I^{(k,l)})$ it outputs the diameter of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired.

The pseudocode for $C_{\text{DIAM}}^G(k, l)$ with $G = A_n$ can be found in Pseudocode 4. From Line 11 onwards the code is identical to Pseudocode 1. The rest of the code is self-explanatory.

Pseudocode 4 $C_{\text{DIAM}}^{A_n}(k, l)$

```
1: define  $a := k$ 
2: define  $b := l$ 
3: define  $G := A_{ab}$ 
4: define  $x := (a!b!)/2$ 
5: define  $max$  to be the set of subgroups of  $G$  of cardinality  $x$ 
6: for  $J$  in  $max$  do
7:   if  $J \cong (S_a \wr S_b) \cap A_{ab}$  then
8:     define  $H := J$ 
9:   end if
10: end for
11: Lines 11 to 81 from Pseudocode 1
```

5.3 $C_{\text{LOW}}(k, l, \sigma)$

In this section we detail the computer program $C_{\text{LOW}}(k, l, \sigma)$ which is used in the proof of Theorem 3.2.6(2). This program takes as inputs integers $k, l > 1$ and a permutation σ as described in the proof. It outputs a lower bound for the diameter of the graph $\Gamma_{[M_{kl}]}$.

The pseudocode for $C_{\text{LOW}}(k, l, \sigma)$ can be found in Pseudocode 5. We now explain the pseudocode. Recall that σ is a permutation which maps A to B , where A and B are some (k, l) -partitions, and any permutation mapping A to B is of the form $w\sigma$, where $w \in G_A \cong S_k \wr S_l$ ($G = S_{kl}$). The method used in the code is to calculate for each permutation g mapping A to B the least number T_g of transpositions g can be a product of. Every time T_g is strictly less than the value in the variable *min*, we re-define *min* to be T_g . The variable *min* is initially set to the value 100; this can be set to any number which is sufficiently large. The least value of T_g , i.e. the value of *min* at the end of the code, is the output. Note that in Line 13, the notation $|c|$ denotes the length of the cycle c .

Pseudocode 5 $C_{\text{LOW}}(k, l, \sigma)$

```
1: define  $a := k$ 
2: define  $b := l$ 
3: define  $G := S_{ab}$ 
4: define  $g_0 := \sigma$ 
5: define  $W := S_a \wr S_b$ 
6: define  $min := 100$ 
7: for  $w$  in  $W$  do
8:   define  $g := w * g_0$ 
9:   define  $h$  to be the cycle decomposition of  $g$ 
10:  define  $numberOfTranspositions := 0$ 
11:  for each cycle  $c$  in  $h$  do
12:    if  $c$  is non-trivial then
13:      add  $(|c| - 1)$  to  $numberOfTranspositions$ 
14:    end if
15:  end for
16:  if  $numberOfTranspositions < min$  then
17:    set  $min := numberOfTranspositions$ 
18:  end if
19: end for
20: output  $min$ 
```

5.4 $C_{\text{VAL}}^G(d, L)$

In this section we detail the computer program $C_{\text{VAL}}^G(d, L)$ for $G = S_n$ and $G = A_n$ which is used in the proof of Proposition 3.5.2 with $d = 5$ and in the proof of Theorem 3.2.8(3) with $d = 2$, and $L = L_{[n]}$. This program takes as inputs an integer $d \geq 1$ and a list L consisting of positive integers n . It outputs the values of n from L for which there exist primitive subgroups H of G satisfying (2.2) from Lemma 2.2.1.

The pseudocode for $C_{\text{VAL}}^G(d, L)$ with $G = S_n$ can be found in Pseudocode 6 and is fairly self-explanatory. The Pseudocode for $G = A_n$ is identical except with Line 3 replaced with ‘**define** $G := A_n$ ’.

Pseudocode 6 $C_{\text{VAL}}^{S_n}(d, L)$

```
1: define  $c := d$ 
2: for  $n$  in  $L$  do
3:   define  $G := S_n$ 
4:   define  $max$  to be the set of maximal subgroups of  $G$ 
5:   for  $H$  in  $max$  do
6:     define  $x := |H|$ 
7:     define  $sum := 1 + 2x + 2x(2x - 1) + \dots + 2x(2x - 1)^{c-1}$ 
8:     if  $H$  is a primitive subgroup of  $G$  and  $|G| \leq sum * x$  and  $H \neq A_n$ 
       then
9:       output  $n$ 
10:    end if
11:  end for
12: end for
```

5.5 $C_{\text{LOW}}^G(d, L)$

In this section we detail the computer program $C_{\text{LOW}}^G(d, L)$ for $G = S_n$ and $G = A_n$ which is used in the proof of Proposition 3.5.2 with $d = 5$ and $L = L_{[n_{\text{new}}]}$. This program takes as inputs an integer $d \geq 1$ and a list L consisting of positive integers n . It outputs the values of n from L for which there exist maximal primitive subgroups H for which the lower bound for the diameter in Proposition 2.2.2 is strictly less than d . It also identifies the subgroups H with pairs of numbers (a, b) which indicate that H is the a^{th} group of degree b in the database of primitive permutation groups in Magma.

The pseudocode for $C_{\text{LOW}}^G(d, L)$ with $G = S_n$ can be found in Pseudocode 7 and is fairly self-explanatory. The Pseudocode for $G = A_n$ is identical except with Line 3 replaced with ‘**define** $G := A_n$ ’.

Pseudocode 7 $C_{\text{LOW}}^{S_n}(d, L)$

```
1: define  $c := d$ 
2: for  $n$  in  $L$  do
3:   define  $G := S_n$ 
4:   define  $max$  to be the set of maximal subgroups of  $G$ 
5:   for  $H$  in  $max$  do
6:     define  $x := |H|$ 
7:     define  $sum := 1 + 2x + 2x(2x - 1) + \dots + 2x(2x - 1)^{d-1}$ 
8:     if  $H$  is a primitive and  $|G| \leq sum * x$  and  $H \neq A_n$  then
9:       define  $S$  to be the set of subgroups of  $H$ 
10:      define an empty list  $K$ 
11:      for  $X$  in  $S$  do
12:        define  $NG := N_G(X)$ 
13:        define  $NH := N_H(X)$ 
14:        if  $|NG| > |NM|$  then
15:          append  $X$  to  $K$ 
16:        end if
17:      end for
18:      define an empty list called  $sizes$ 
19:      for  $X$  in  $K$  do
20:        append  $|X|$  to  $sizes$ 
21:      end for
22:      for  $i$  in  $sizes$  do
23:        if  $sizes[i]$  is the maximum value in  $sizes$  then
24:          define  $j := i$ 
25:        end if
26:      end for
27:      define  $X := K[j]$ 
28:      define  $m := \frac{\log(|G|/|H|)}{\log(2|H|/|X|)} - 1$ 
29:      define  $NG := N_G(X)$ 
30:      define  $NH := N_H(X)$ 
```

```

31:         for  $g$  in  $NG$  do
32:             if  $g$  is not in  $NH$  then
33:                 if  $g$  has order 2 then
34:                     set  $m := \frac{\log(|G|/|H|)}{\log(|H|/|X|)} - 1$ 
35:                     break  $g$ 
36:                 end if
37:             end if
38:         end for
39:         if  $m < c$  then
40:             identify  $H$  with a pair  $(a, b)$ 
41:             output  $n$  and the  $a$ th group of degree  $b$  from the database
              of primitive permutation groups
42:         end if
43:     end if
44: end for
45: end for

```

Note that Lines 9 to 38 only require a group G and maximal subgroup H to be defined, and thus we can re-use this part of the pseudocode whenever we have such a G and H .

5.6 $C_{\text{DIAM}}^G(d, L)$

In this section we detail the computer program $C_{\text{DIAM}}^G(d, L)$ for $G = S_n$ and $G = A_n$ which is used in the proof of Theorem 3.2.6(3) with $d = 5$, and in the proof of Theorem 3.2.8(3) with $d = 2$, and $L = L_{[n_{\text{new}}]}$. This program takes as inputs an integer $d \geq 1$ and a list L consisting of positive integers n . For each primitive subgroup H of G satisfying (2.2) from Lemma 2.2.1, it outputs the rank of $(G, (G : H))$ and for each orbital of the action, it outputs the diameter and valency of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired. The latter is useful information when counting the number of orbital graphs that occur; the orbital graph associated with each orbital that is not self-paired occurs

twice (a second time with the paired orbital), and thus has to be counted only once. The code also identifies the subgroups H with pairs of numbers (a, b) which indicate that H is the a^{th} group of degree b in the database of primitive permutation groups in Magma.

The pseudocode for $C_{\text{DIAM}}^G(d, L)$ with $G = S_n$ can be found in Pseudocode 8 and is fairly self-explanatory. The Pseudocode for $G = A_n$ is identical except with Line 3 replaced with ‘**define** $G := A_n$ ’.

Pseudocode 8 $C_{\text{DIAM}}^{S_n}(d, L)$

```

1: define  $c := d$ 
2: for  $n$  in  $L$  do
3:   define  $G := S_n$ 
4:   define  $max$  to be the set of maximal subgroups of  $G$ 
5:   for  $H$  in  $max$  do
6:     define  $x := |H|$ 
7:     define  $sum := 1 + 2x + 2x(2x - 1) + \dots + 2x(2x - 1)^{c-1}$ 
8:     if  $H$  is a primitive subgroup of  $G$  and  $|G| \leq sum * x$  and  $H \neq A_n$ 
       then
9:       identify  $H$  with a pair  $(a, b)$ 
10:      output  $n$  and the  $a^{\text{th}}$  group of degree  $b$  from the database
        of primitive permutation groups
11:      Lines 11 to 81 from Pseudocode 1, with the extra output
        valency in Line 78
12:    end if
13:  end for
14: end for

```

5.7 $C_{\text{LOW}}^{G,H}(d, L)$

In this section we detail the computer program $C_{\text{LOW}}^{G,H}(d, L)$ which is used in the proof of Proposition 4.6.4 with $d = 2$ and $L = L_{[q_{\text{old}}]}$. This program takes as inputs an integer $d \geq 1$ and a list L consisting of prime powers q . It outputs the values of q from L for which the lower bound for the diameter in Proposition 2.2.2 is strictly less than d .

The pseudocode for $C_{\text{LOW}}^{G,H}(d, L)$ with $(G, H) = (\text{PSL}_2(q), A_4)$ can be found in Pseudocode 9 and is fairly self-explanatory.

Pseudocode 9 $C_{\text{LOW}}^{\text{PSL}_2(q), A_4}(d, L)$

```

1: define  $c := d$ 
2: define an empty list called remainingValues
3: for  $q$  in  $L$  do
4:   define  $G := \text{PSL}_2(q)$ 
5:   define  $max$  to be the set of maximal subgroups of  $G$  with order  $|A_4|$ 
6:   for  $H$  in  $max$  do
7:     if  $H \cong A_4$  then
8:       Lines 9 to 38 from Pseudocode 7
9:       if  $m < c$  then
10:        append to  $q$  to remainingValues
11:      end if
12:    end if
13:  end for
14: end for
15: output remainingValues

```

The pseudocode for $C_{\text{LOW}}^{G,H}(d, L)$ with $(G, H) = (\text{PSL}_2(q) \cdot \langle \ddot{\delta} \rangle, A_4 \cdot \langle \ddot{\delta} \rangle)$ can be found in Pseudocode 10. Recall that $\text{PGL}_2(q) = \text{PSL}_2(q) \cdot \langle \ddot{\delta} \rangle$ and therefore it suffices to define $G := \text{PGL}_2(q)$. The task of defining the subgroup H requires a little more complicated code compared to that in Pseudocode 9; we define H to be the maximal subgroup of G which contains A_4 and satisfies $H/A_4 = \langle \ddot{\delta} \rangle$ (Lines 5 to 10). After H is defined, the rest of the code is fairly self-explanatory.

Pseudocode 10 $C_{\text{LOW}}^{\text{PSL}_2(q) \cdot \langle \ddot{\phi} \rangle, A_4 \cdot \langle \ddot{\phi} \rangle}(d, L)$

```

1: define  $c := d$ 
2: define an empty list called remainingValues
3: for  $q$  in  $L$  do
4:   define  $G := \text{PGL}_2(q)$ 
5:   define  $max$  to be the set of maximal subgroups of  $G$  with order  $2|A_4|$ 
6:   define  $\Gamma := \text{PGL}_2(q)/\text{soc}(\text{PGL}_2(q))$ 
7:   for  $H$  in  $max$  do
8:     define  $S$  to be the set of subgroups of  $H$ 
9:     for  $J$  in  $S$  do
10:      if  $J \cong A_4$  and  $H/J = \Gamma$  then
11:        Lines 9 to 38 from Pseudocode 7
12:      if  $m < c$  then
13:        append  $q$  to remainingValues
14:      end if
15:    end if
16:  end for
17: end for
18: end for
19: output remainingValues

```

The pseudocode for $C_{\text{LOW}}^{G,H}(d, L)$ with $(G, H) = (\text{PSL}_2(q), A_5)$ is identical to Pseudocode 9 except with A_4 replaced by A_5 . The pseudocode for $(G, H) = (\text{PSL}_2(q) \cdot \langle \ddot{\phi} \rangle, A_5 \cdot \langle \ddot{\phi} \rangle)$ can be found in Pseudocode 11. The task of defining G and H in this code is a bit more complex. For a given value of $q = p^2$ where $p \equiv \pm 3 \pmod{10}$, there are multiple groups J with $\text{soc}(J) = \text{PSL}_2(q)$ and $J/\text{soc}(J) \cong \langle \ddot{\phi} \rangle$, however by Table 4.1, only one of these will contain a maximal subgroup of order $2|A_5|$. We use this fact to define G in Lines 4 to 18 (note that $\text{Aut}(\text{PSL}_2(q))$ is frequently denoted by $\text{PTL}_2(q)$). The maximal subgroup H is defined in a similar way to that in Pseudocode 10.

Pseudocode 11 $C_{\text{LOW}}^{\text{PSL}_2(q) \cdot \langle \ddot{\phi} \rangle, A_5 \cdot \langle \ddot{\phi} \rangle}(d, L)$

```

1: define  $c := d$ 
2: define an empty list called remainingValues
3: for  $q$  in  $L$  do
4:   define  $A := \text{P}\Gamma\text{L}_2(q)$ 
5:   define  $\Gamma := A/\text{PGL}_2(q)$ 
6:   define an empty set called possibleGroups
7:   define  $S$  to be the set of subgroups of  $A$ 
8:   for  $G$  in  $S$  do
9:     if  $\text{soc}(G) = \text{PSL}_2(q)$  and  $G/\text{soc}(G) \cong \Gamma$  then
10:      include  $G$  in possibleSubgroups
11:    end if
12:  end for
13:  for  $J$  in possibleGroups do
14:    define  $M$  to be the set of maximal subgroups of  $J$  of order  $2|A_5|$ 
15:    if  $M$  is non-empty then
16:      define  $G := J$ 
17:    end if
18:  end for
19:  define  $\text{max}$  to be the set of maximal subgroups of  $G$  of order  $2|A_5|$ 
20:  for  $S$  in  $\text{max}$  do
21:    define  $T$  to be the set of subgroups of  $S$ 
22:    for  $J$  in  $T$  do
23:      if  $J \cong A_5$  and  $S/J = \Gamma$  then
24:        define  $H := S$ 
25:        Lines 9 to 38 from Pseudocode 7
26:        if  $m < c$  then
27:          append  $q$  to remainingValues
28:        end if
29:      end if
30:    end for
31:  end for
32: end for

```

The pseudocode for $C_{\text{LOW}}^{G,H}(d, L)$ with $(G, H) = (\text{PSL}_2(q), S_4)$ is identical to Pseudocode 9 except with A_4 replaced by S_4 .

5.8 $C_{\text{DIAM}}^{G,H}(q)$

In this section we detail the computer program $C_{\text{DIAM}}^{G,H}(q)$ which is used in the proof of Theorem 4.6.1(2) and (3). This program takes as input a prime power q . For G and H as in Section 5.7, it outputs the rank of $(G, (G : H))$ and for each orbital of the action, it outputs the diameter and valency of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired.

The pseudocode for a particular choice of G and H will involve defining G and H and then computing the diameters of the orbital graphs. We can define G and H using one of the pseudocodes in Section 5.7 and we can compute the diameters of the orbital graphs using Lines 11 to 81 from Pseudocode 1. Thus the pseudocode for $C_{\text{DIAM}}^{G,H}(q)$ is just a concatenation of previous pseudocodes.

Note that for some of the groups G defined in Sections 5.7 there are two conjugacy classes of maximal subgroups isomorphic to H , however, when constructing the set of maximal subgroups of G in Magma, a pre-defined function is used which produces all conjugacy class representatives. In this way, the codes mentioned in this chapter, output results for both conjugacy classes.

5.9 $C_{\text{DIAM}}^{\text{PSL}_2}(q)$

In this section we detail the computer program $C_{\text{DIAM}}^{\text{PSL}_2}(q)$ which is used to give the output in Table 4.2. This program takes as input a prime power q . It outputs the rank of $(G, (G : H))$ where $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $S \not\leq H <_{\max} G$, and for each orbital of the action, it outputs the diameter and valency of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired. It also outputs the groups G and H with their orders.

The pseudocode for $C_{\text{DIAM}}^{\text{PSL}_2}(q)$ can be found in Pseudocode 12 and is fairly self-explanatory.

Pseudocode 12 $C_{\text{DIAM}}^{\text{PSL}_2}(q)$

```

1: define  $t := q$ 
2: define  $sub$  to be the set of subgroups of  $\text{P}\Gamma\text{L}_2(t)$ 
3: for  $G$  in  $sub$  do
4:   if  $\text{soc}(G) = \text{PSL}_2(t)$  then
5:     define  $max$  to be the set of maximal subgroups of  $G$ 
6:     for  $H$  in  $max$  do
7:       if  $\text{PSL}_2(t) \not\leq H$  then
8:         output  $G$  and  $H$ 
9:         Lines 11 to 81 from Pseudocode 1, with the extra output
            $valency$  in Line 78
10:      end if
11:    end for
12:  end if
13: end for

```

5.10 $C_{\text{D}\pm}^{\text{PSL}_2}(q)$

In this section we detail the computer program $C_{\text{D}\pm}^{\text{PSL}_2}(q)$ which contributes to the output in Table 4.2. This program takes as input a prime power q . It outputs the rank of $(G, (G : H))$ where $S := \text{soc}(G) \cong \text{PSL}_2(q)$ and $S \not\leq H <_{\max} G$ with $H \cap S \cong D_{q\pm 1}$, and for each orbital of the action, it outputs the diameter and valency of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired. It also outputs the groups G and H with their orders.

The pseudocode for $C_{\text{D}\pm}^{\text{PSL}_2}(q)$ can be found in Pseudocode 13 and is fairly self-explanatory.

Pseudocode 13 $C_{D\pm}^{\text{PSL}_2}(q)$

```

1: define  $t := q$ 
2: define  $sub$  to be the set of subgroups of  $\text{P}\Gamma\text{L}_2(t)$ 
3: for  $G$  in  $sub$  do
4:   if  $\text{soc}(G) = \text{PSL}_2(t)$  then
5:     define  $\Gamma := G/\text{soc}(G)$ 
6:     define  $max$  to be the set of maximal subgroups of  $G$ 
7:     for  $H$  in  $max$  do
8:       if  $\text{PSL}_2(t) \not\leq H$  then
9:         output  $G$  and  $H$ 
10:        define  $S$  to be the set of all normal subgroups of  $H$ 
11:        define  $x := (t \pm 1)/2$ 
12:        for  $K$  in  $S$  do
13:          if  $K \cong D_{t\pm 1}$  and  $H/K = \Gamma$  then
14:            Lines 11 to 81 from Pseudocode 1, with the extra
            output valency in Line 78
15:          end if
16:        end for
17:      end if
18:    end for
19:  end if
20: end for

```

5.11 $C_{\text{DIAM}}^{\text{PGL}_2}(q)$

In this section we detail the computer program $C_{\text{DIAM}}^{\text{PGL}_2}(q)$ which contributes to the output in Table 4.2. This program takes as input a prime power q . It outputs the rank of $(G, (G : H))$ where $G = \text{PGL}_2(q)$ and $\text{PSL}_2(q) \not\leq H <_{\max} G$, and for each orbital of the action, it outputs the diameter and valency of the corresponding orbital graph as well as ‘true’ or ‘false’ depending on whether or not the orbital is self-paired. It also outputs the groups G and H with their orders.

The pseudocode for $C_{\text{DIAM}}^{\text{PGL}_2}(q)$ can be found in Pseudocode 14 and is fairly self-explanatory.

Pseudocode 14 $C_{\text{DIAM}}^{\text{PGL}_2}(q)$

```
1: define  $t := q$ 
2: define  $G := \text{PGL}_2(q)$ 
3: define  $max$  to be the set of maximal subgroups of  $G$ 
4: for  $H$  in  $max$  do
5:   if  $\text{PSL}_2(t) \not\leq H$  then
6:     output  $G$  and  $H$ 
7:     Lines 11 to 81 from Pseudocode 1, with the extra output valency
       in Line 78
8:   end if
9: end for
```

Chapter 6

Parabolic actions of the simple groups of Lie type

In this chapter we analyse the orbital diameters of the simple groups of Lie type. In particular, we describe the *parabolic actions* for which the orbital diameter is at most 2. For the simple classical groups we also produce an infinite family of orbital graphs of diameter 2.

In Section 6.1, we detail the background material necessary for the chapter and in Section 6.2 we state the main results of the chapter. In Sections 6.3 and 6.4, we describe the maximal parabolic subgroups of the simple classical groups and the orbital graphs of the corresponding parabolic actions. In Sections 6.5 and 6.6, we give proofs of the main results of the chapter.

6.1 Preliminary theory

In this section we detail the background material which will be needed in the chapter.

We begin by describing *parabolic subgroups* of groups with (B, N) -pairs. The following theory can be found in Chapter 8 of [5].

Definition 6.1.1. Let G be a group. A pair (B, N) of subgroups of G is called a (B, N) -pair if the following hold:

1. G is generated by B and N ;
2. $B \cap N$ is a normal subgroup of N ;
3. The group $W := \frac{N}{B \cap N}$ is generated by a set of elements $w_i, i \in I$, such that $w_i^2 = 1$;
4. For $n_i \in N$, if n_i maps to w_i under the natural homomorphism, and $n \in N$, then

$$Bn_iB.BnB \subseteq Bn_inB \cup BnB;$$

5. If n_i is as above, then $n_iBn_i \neq B$.

The group W as defined above is called the *Weyl* group of G , the elements w_i are called *simple reflections*, and the cardinality of the set I is called the *rank* of W .

Proposition 6.1.2 (Proposition 8.2.2 in [5]). *Let G be a group with a (B, N) -pair. Then the following hold:*

1. $G = BNB$.
2. For each subset $J \subseteq I$, let W_J be the subgroup of W generated by the elements w_i for $i \in J$, and let N_J be the subgroup of N mapping to W_J under the natural homomorphism. Then $P_J := BN_JB$ is a subgroup of G .

Definition 6.1.3. Let G be a group with (B, N) -pair. A *parabolic subgroup* of G is a subgroup H which contains gBg^{-1} for some $g \in G$.

The subgroups P_J from Proposition 6.1.2 certainly contain B and are thus parabolic subgroups by definition. The next result follows from Theorems 8.3.2 and 8.3.3 in [5] and shows that in fact, up to conjugacy, these are the only parabolic subgroups.

Proposition 6.1.4. *Let G be a group with a (B, N) -pair. Every parabolic subgroup of G is conjugate in G , to some P_J where $J \subseteq I$. Furthermore, the subgroups P_J for distinct subsets $J \subseteq I$ are all distinct and non-conjugate in G .*

We now describe the parabolic subgroups which are maximal.

Definition 6.1.5. Let G be a group with a (B, N) -pair. A *maximal* parabolic subgroup of G is a subgroup which is conjugate to $P_i := P_J$, where $J := I \setminus \{i\}$ for some $i \in I$. We will denote the corresponding subgroup W_J of the Weyl group W by W_i . A *parabolic action* of G is the natural action of G on the set $(G : H)$ where H is a maximal parabolic subgroup of G .

Remark 6.1.6. Let G be a group with (B, N) -pair. Since all the maximal parabolic subgroups are conjugate to P_k for some k , in order to analyse the orbital diameters of the maximal parabolic actions of G , it suffices to analyse the actions of G on $(G : P_k)$. Thus, henceforth we will assume that a maximal parabolic subgroup of G is equal to P_k for some k .

There are plenty of groups which possess (B, N) -pairs. For the results in the thesis, we will only require existence of (B, N) -pairs for the classical groups and exceptional groups. Explicit constructions for (B, N) -pairs for the classical groups can be found in [24, p. 46, 62, 67, 74], which justify the fact that the groups $\mathrm{SL}_n(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{SU}_n(q)$ and $\Omega_n^\epsilon(q)$ ($\epsilon \in \{\circ, +, -\}$) all possess (B, N) -pairs.

Definition 6.1.7. Let $G := \mathrm{PX}_n(q) = X_n(q)/Z$ be a simple classical group, where Z is the centre of $X_n(q)$. We define a parabolic subgroup of G to be P/Z , where P is a parabolic subgroup of $X_n(q)$.

Remark 6.1.8. We shall see later on that parabolic subgroups of the classical groups are stabilisers of certain types of subspaces of the underlying vector space, under the natural actions of the classical groups. Now, the centre Z of a classical group $X_n(q)$ is a subset of scalar matrices (see [24, p. 44, 61, 66, 70])

and any scalar matrix stabilises a subspace, so a parabolic subgroup of $X_n(q)$ always contains Z . Thus the natural action of $X_n(q)$ on induces a natural action of $PX_n(q)$. The maximal parabolic subgroups of the simple classical groups are thus also the stabilisers of certain types of subspaces of the underlying vector spaces; we shall keep the notation P_k for the maximal parabolic subgroups of the simple classical groups.

The exceptional groups (of Lie type) are defined with respect to a prime power q and consist of the exceptional groups denoted $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$ ($q \geq 3$), the *twisted exceptional groups*, denoted ${}^2E_6(q)$, ${}^3D_4(q)$, ${}^2F_4(2^{2m+1})$ ($m \geq 1$), ${}^2B_2(2^{2m+1})$ ($m \geq 1$), ${}^2G_2(3^{2m+1})$ ($m \geq 1$), and the *Tits group* ${}^2F_4(2)'$. We will see that it is not actually required to define the exceptional groups for the purposes of the results in this chapter. It is a fact that all exceptional groups (excluding the Tits group) possess (B, N) -pairs; see [5, p. 108, 227].

6.2 Statements of the main results

We now state the main results of this chapter. They are split into two results; one concerning the simple classical groups and one concerning the exceptional groups.

Theorem 6.2.1. *Let (G, Y) be a primitive permutation group where $G := PX_n(q)$ is a simple classical group with $X \in \{\text{SL}, \text{Sp}, \text{SU}, \Omega^\circ, \Omega^\pm\}$, and $Y := (G : P_k)$, where P_k is maximal parabolic subgroup of G . Then*

1. $\text{diam}_O(G, Y) \leq 2$ if and only if
 - (a) $k = 1$ (or $k = n - 1$ if $X_n = \text{SL}_n$), or
 - (b) X_n and k are in Table 6.1.

$\mathbf{X}_n$	$\mathbf{k}$
SL_n	P_2, P_{n-2}
Sp_4	P_2
$\mathrm{SU}_4, \mathrm{SU}_5$	P_2
Ω_5, Ω_6^-	P_2
$\Omega_6^+, \Omega_8^+, \Omega_{10}^+$	P_k for $k = n-1, n$

Table 6.1: Pairs (X_n, k) ($k \neq 1$) such that $\mathrm{diam}_O(G, Y) \leq 2$, where $G := \mathrm{PX}_n(q)$ and $Y := (G : P_k)$

2. (G, Y) has an orbital graph of diameter 2, except for when (X_n, k) is one of the following (in which case the rank of the action is 2):

- $(\mathrm{SL}_n, 1), (\mathrm{SL}_n, n-1)$
- $(\mathrm{Sp}_2, 1)$
- $(\mathrm{SU}_2, 1), (\mathrm{SU}_3, 1)$
- $(\Omega_3, 1), (\Omega_4^-, 1), (\Omega_6^+, 3)\}$.

Remark 6.2.2. We will see that part 1 of Theorem 6.2.1 is just a concatenation of results that already exist in previous literature, however to the best of our knowledge, finding orbital graphs of diameter 2 in part 2 is a result which is not extractable from existing literature.

Let (G, Y) be as in Theorem 6.2.1. Recall that the converse of Theorem 1.2.8(1) asserts that if we let n tend to infinity, then $\mathrm{diam}_O(G, Y)$ will be bounded above by some fixed constant provided that k is bounded. We conjecture the following values for $\mathrm{diam}_O(G, Y)$ for a special case of (G, Y) .

Conjecture 6.2.3. *Let (G, Y) be a primitive permutation group where $G := \mathrm{P}\mathrm{Sp}_{2n}(q)$, and $Y := (G : P_k)$, where P_k is maximal parabolic subgroup of G . Then*

$$\mathrm{diam}_O(G, Y) = \begin{cases} n, & \text{if } n \leq 2k \\ 2k, & \text{if } n \geq 2k. \end{cases}$$

Remark 6.2.4. The case $n = k$ of Conjecture 6.2.3 can be easily proved as follows. Suppose $n = k$. By Lemma 6.4.2(1), the rank of (G, Y) is $k + 1$. Now, the diameter of any orbital graph is bounded above by the rank of the action minus one, and thus $\text{diam}_O(G, Y) \leq k$. Moreover, (G, Y) has an orbital graph of diameter k by Table 6.2 from Lemma 6.5.8, which proves the equality.

Theorem 6.2.5. *Let (G, X) be a primitive permutation group with G an exceptional group of Lie type ($G \neq {}^2F_4(2)'$) and $X := (G : P_k)$, where P_k is a maximal parabolic subgroup of G . Then $\text{diam}_O(G, X) \leq 2$ if and only if $G = E_6(q)$ and $k = 1, 6$, or $G = {}^2B_2(2^{2m+1})$, or $G = {}^2G_2(3^{2m+1})$.*

6.3 Maximal parabolic subgroups of the simple classical groups

In this section we will describe the maximal parabolic subgroups of the simple classical groups.

We begin with the linear groups; see Section 3.3.3 in [24] for the next result.

Proposition 6.3.1. *The natural action of $G := \text{SL}_n(q)$ on the set V_k of k -subspaces of the underlying vector space, is transitive. The maximal parabolic subgroups of G are P_k for $k \leq n$ and P_k is the stabiliser in G of a k -subspace.*

Remark 6.3.2. Observe that the actions of $\text{PSL}_n(q)$ on V_k and V_{n-k} are equivalent and thus henceforth we will assume that $k \leq n/2$ for this case.

We now describe the parabolic subgroups of the remaining simple classical groups. Recall the definition of a totally singular subspace (Definition 2.3.13); we add to this definition below.

Definition 6.3.3. Let (V, f) be a symplectic or unitary space, and let (V, Q) be a quadratic space.

1. A vector $v \in V$ is called *isotropic* if $(v, v) = 0$, and *singular* if $Q(v) = 0$.
2. A subspace $W \leq V$ is called *totally isotropic* if $(w, w) = 0$ for all $w \in W$, and *totally singular* if $Q(w) = 0$ for all $w \in W$.
3. For a subspace $W \leq V$, we define $\text{Rad}(W) := W \cap W^\perp$.

For the next result, see Sections 3.5.4 and 3.6.2 in [24].

Proposition 6.3.4. *Let $G := X_n(q)$ be a classical group, where X belongs to the set $\{\text{Sp}, \text{SU}, \Omega^\epsilon(\epsilon = \circ, -)\}$. The natural action of G on the set V_k of all totally isotropic (or totally singular if $X = \Omega^\epsilon$) k -subspaces of the underlying vector space, is transitive. The maximal parabolic subgroups of G are P_k , where*

1. $k \leq \frac{n}{2}$ for $X = \text{Sp}, \text{SU}, \Omega^\circ$;
2. $k \leq \frac{n}{2} - 1$ for $X = \Omega^-$,

and P_k is the stabiliser of a totally isotropic (or totally singular) k -subspace.

For the next result see Section 3.7.4 in [24] and Lemma 2.5.8(ii) in [14].

Proposition 6.3.5. *The natural action of $G := \Omega_{2n}^+(q)$ on the set V_k of all totally singular k -subspaces of the underlying vector space, is transitive for $k \leq n - 1$. If $k = n$, then G has 2 orbits on V_n where two totally singular subspaces U and W of dimension n are in the same orbit if and only if $n - \dim(U \cap W)$ is even; let V_n^1 and V_n^2 denote the two orbits. The maximal parabolic subgroups of G are P_k for $k \leq n$. For $k \leq n - 2$, P_k is the stabiliser of a totally singular k -subspace, and for $k = n - 1$ and $k = n$, P_k is the stabiliser of a totally singular n -subspace in V_n^1 and V_n^2 , respectively.*

Remark 6.3.6. The actions of $G := \mathrm{P}\Omega_{2n}^+(q)$ on cosets of the two parabolic subgroups P_{n-1} and P_n are permutation isomorphic and thus to analyse the corresponding orbital diameters, it suffices to analyse any one of the parabolic actions. To see this, one may proceed similarly to Remark 4.4.3 in Chapter 4; the two orbits V_n^1 and V_n^2 fuse under the action of $\mathrm{PO}_{2n}^+(q)$ (see Section 3.7.4 in [24]). This yields an automorphism of G and a bijection between the two orbits which form a permutation isomorphism between the two actions. On this note, henceforth we shall not analyse the parabolic subgroup P_{n-1} and we will denote V_n^2 by V_n .

Note that we have used the notation V_k and P_k to denote different sets and groups in Propositions 6.3.1, 6.3.4 and 6.3.5. We will continue to use this notation; the set V_k and the group P_k should be clear from the classical group in question.

We conclude this section by stating a result which will be very useful when calculating the ranks of some of the parabolic actions described above. The result follows from the fact that, for a group G with a (B, N) -pair and Weyl group W , there is a bijection between the suborbits of the action of G on $(G : P_J)$ and the action of W on $(W : W_J)$ (see Theorem 10.5.1(iii) in [4]). Notice that suborbits of the action of G on $(G : P_J)$ are double cosets $P_J x P_J$, where $x \in G$. Now recall that $G = BNB$ and $P_J = BN_J B$, and thus we may suppose $x \in N$. Further, for any $y \in w := x(B \cap N)$, we have $P_J x P_J = P_J y P_J$, and thus we will write $P_J w P_J$ to mean the double coset $P_J x P_J$ for any $x \in w$.

Lemma 6.3.7. *Let G be a group with a (B, N) -pair and Weyl group W , and let P_J be a parabolic subgroup of G . There is a 1-1 correspondence between the suborbits of the action of G on $(G : P_J)$ and the action of W on $(W : W_J)$, where the suborbit $W_J w W_J$ corresponds to the suborbit $P_J w P_J$. Thus the rank of the action of G on $(G : P_J)$ is equal to the rank of the action of W on $(W : W_J)$.*

Remark 6.3.8. If $G := \text{PX}_n(q) = X_n(q)/Z$ is a simple classical group with parabolic subgroup $H := P_J/Z$, then the rank of the action of G on $(G : H)$ is equal to the rank of the action of $X_n(q)$ on $(X_n(q) : P_J)$ and thus by Lemma 6.3.7 is equal to the rank of the action of W on $(W : W_J)$.

6.4 Orbital graphs of the parabolic actions of the simple classical groups

In order to prove part 2 of Theorem 6.2.1, we need to determine the orbitals and orbital graphs of the parabolic actions of the simple classical groups, which we do next.

Proposition 6.4.1. *Let (G, Y) be a primitive permutation group where $G := \text{PSL}_n(q)$ and $Y := (G : P_k)$, where P_k is a maximal parabolic subgroup of G and $k \leq n/2$. The action of G on Y is equivalent to the natural action of G on the set V_k . The non-diagonal orbitals of (G, V_k) are*

$$\Delta_i := \{(A, B) \in V_k^2 : \dim(A \cap B) = i\}, \quad i \in \{0, \dots, k-1\}.$$

Proof. The first statement follows from Proposition 6.3.1. It is easy to see that the sets Δ_i are non-empty, disjoint and that their union (together with the diagonal orbital) is V_k^2 . It is also clear that if (A, B) and (C, D) are two elements of V_k^2 which are in the same non-diagonal orbital of (G, V_k) , then $\dim(A \cap B) = \dim(C \cap D)$.

It remains to show that G is transitive on the sets Δ_i . Suppose (A, B) and (C, D) are in Δ_i . Let U be a basis of $A \cap B$ and let W be a basis of $C \cap D$. Extend U to a basis U_A of A and U_B of B . Similarly define W_C and W_D . Then $B_1 := U_A \cup U_B$ and $B_2 := W_C \cup W_D$ form bases for $A + B$ and $C + D$, respectively. Now extend B_1 and B_2 to bases B'_1 and B'_2 of the underlying vector space; the map g which maps B'_1 to B'_2 point-wise is an element of $\text{GL}_n(q)$ which maps (A, B) to (C, D) . Now, observe that we

can pick $h \in \mathrm{GL}_n(q)$ mapping A to A and B to B , with $\det(h) = \det(g)^{-1}$. Thus $\det(gh) = 1$ and gh maps (A, B) to (C, D) . $\square$

To determine the orbitals for the parabolic actions of the remaining simple classical groups, we will use the ranks of these actions. These ranks have been computed in previous literature and we state them next; here we will write $(\mathrm{PX}_n(q), P_k)$ to mean the permutation group $(\mathrm{PX}_n(q), Y)$, where $Y := (\mathrm{PX}_n(q) : P_k)$.

Lemma 6.4.2. *The ranks of the parabolic actions of the simple classical groups are as follows.*

1. *The rank of the groups (PSp_{2n}, P_k) , $(\mathrm{PSU}_{2n}(q), P_k)$, $(\mathrm{PSU}_{2n+1}(q), P_k)$, $(\mathrm{P}\Omega_{2n+1}(q), P_k)$, and $(\mathrm{P}\Omega_{2n+2}^-(q), P_k)$ (for $k \leq n$) is*

$$\begin{cases} \frac{(n-k+1)(3k-n+2)}{2}, & n \leq 2k \\ \frac{(k+1)(k+2)}{2}, & n \geq 2k. \end{cases}$$

2. *The rank of $(\mathrm{P}\Omega_{2n}^+(q), P_k)$ (for $k \leq n-2$) is*

$$\begin{cases} 1 + \frac{(n-k+2)(3k-n+1)}{2}, & n \leq 2k \\ \frac{(k+1)(k+2)}{2}, & n > 2k. \end{cases}$$

3. *The rank of $(\mathrm{P}\Omega_{2n}^+(q), P_n)$ is*

$$\begin{cases} \frac{n-1}{2} + 1, & n \text{ odd} \\ \frac{n}{2} + 1, & n \text{ even}. \end{cases}$$

Proof. Let W be the Weyl group of the underlying classical group. The action of W on $(W : W_k)$ has rank exactly as in the statement of the lemma (see Proposition 10.4.3 in [4]; see (iii) and (iv) for (1), (vi) for (2) and (v) for (3)). Thus the proof is complete by Lemma 6.3.7. $\square$

Remark 6.4.3. One can easily check using Proposition 6.4.1 and Lemma 6.4.2 that the only parabolic actions of the simple classical groups which have rank 2 are the ones stated in part 2 of Theorem 6.2.1.

We can now determine the orbitals of the parabolic actions of the remaining simple classical groups.

Proposition 6.4.4. *Let (G, Y) be a primitive permutation group where $G := \mathrm{PSp}_{2n}(q), \mathrm{PSU}_{2n}(q), \mathrm{PSU}_{2n+1}(q), \mathrm{P}\Omega_{2n+1}(q)$ or $\mathrm{P}\Omega_{2n+2}^-(q)$ and $Y := (G : P_k)$, where P_k is a maximal parabolic subgroup of G . The action of G on Y is equivalent to the natural action of G on the set V_k . For non-negative integers i, j , let*

$$\Delta_{ij} := \{(A, B) \in V_k^2 : \dim(A \cap B) = j, \dim(\mathrm{Rad}(A + B)) = j + 2i\}.$$

If $n \leq 2k$, then the non-diagonal orbitals of (G, V_k) are Δ_{ij} where $i \in \{0, \dots, n - k\}$, and

$$\begin{cases} j \in \{0, \dots, k - 1\}, & i = 0 \\ j \in \{0, \dots, k - i\}, & i \in \{1, \dots, n - k\}. \end{cases}$$

If $n \geq 2k$, then the non-diagonal orbitals of (G, V_k) are Δ_{ij} where $i \in \{0, \dots, k\}$, and

$$\begin{cases} j \in \{0, \dots, k - 1\}, & i = 0 \\ j \in \{0, \dots, k - i\}, & i \in \{1, \dots, k\}. \end{cases}$$

Proof. The first statement in the result follows from Proposition 6.3.4. We claim that for i, j as in the statement of the result, the sets Δ_{ij} are non-empty.

Indeed, let

$$\begin{aligned} U &:= \langle e_1, \dots, e_k \rangle, \\ W &:= \langle e_1, \dots, e_j, e_{k+1}, \dots, e_{k+i}, f_{j+1}, \dots, f_{k-i} \rangle, \end{aligned}$$

where e_i, f_i are the standard basis vectors. Then $(U, W) \in \Delta_{ij}$. It is clear that the sets Δ_{ij} are disjoint. Now suppose (A, B) and (C, D) are two distinct elements of V_k^2 which are in the same orbital. It is easy to see that $\dim(A \cap B) = \dim(C \cap D)$ and $\dim(\text{Rad}(A + B)) = \dim(\text{Rad}(C + D))$. This implies that the rank of the action is at least one more than the total number of Δ_{ij} , which by counting is

$$\begin{cases} \frac{(n-k+1)(3k-n+2)}{2}, & n \leq 2k \\ \frac{(k+1)(k+2)}{2}, & n \geq 2k. \end{cases}$$

In fact, the rank is precisely as above by Lemma 6.4.2(1). Thus, the non-diagonal orbitals are precisely the Δ_{ij} described in the statement. $\square$

Proposition 6.4.5. *Let (G, Y) be a primitive permutation group where $G := \text{P}\Omega_{2n}^+(q)$, $Y := (G : P_k)$, and P_k is maximal parabolic subgroup of G with $k \leq n - 2$. The action of G on Y is equivalent to the natural action of G on the set V_k . Let Δ_{ij} be as in Proposition 6.4.4. If $n > 2k$, the non-diagonal orbitals of (G, V_k) are Δ_{ij} where $i \in \{0, \dots, k\}$, and*

$$\begin{cases} j \in \{0, \dots, k-1\}, & i = 0 \\ j \in \{0, \dots, k-i\}, & i \in \{1, \dots, k\}. \end{cases}$$

If $n \leq 2k$, the non-diagonal orbitals of (G, V_k) are Δ_{ij} where

$i \in \{0, \dots, n - k - 1\}$, and

$$\begin{cases} j \in \{0, \dots, k - 1\}, & i = 0 \\ j \in \{0, \dots, k - i\}, & i \in \{1, \dots, n - k - 1\}, \end{cases}$$

and $\Delta_{n-k,j}$ splits into two orbitals $\Delta_{n-k,j}^+ := (A, B^+)^G$ and $\Delta_{n-k,j}^- := (A, B^-)^G$ of (G, V_k) , for $j \in \{0, \dots, 2k - n\}$, where

$$\begin{aligned} A &:= \langle e_1, \dots, e_k \rangle, \\ B^+ &:= \langle e_1, \dots, e_j, e_{k+1}, \dots, e_n, f_{j+1}, \dots, f_{2k-n} \rangle, \\ B^- &:= \langle e_1, \dots, e_j, e_{k+1}, \dots, e_{n-1}, f_n, f_{j+1}, \dots, f_{2k-n} \rangle. \end{aligned}$$

Proof. The first statement follows from Proposition 6.3.5. The sets described in the statement are non-empty as in the proof of Proposition 6.4.4. Now suppose (A, B) and (C, D) are two distinct elements of V_k^2 which are in the same orbital. It is easy to see that $\dim(A \cap B) = \dim(C \cap D)$ and $\dim(\text{Rad}(A + B)) = \dim(\text{Rad}(C + D))$. Then the proof for $n > 2k$ goes as in the proof of Proposition 6.4.4 since the rank for this case is unchanged by Lemma 6.4.2(2).

Now suppose $n \leq 2k$. By counting the number of orbitals described in the statement plus the diagonal orbital, we obtain

$$1 + k + \left(\sum_{i=1}^{n-k-1} k - i + 1 \right) + 2(2k - n + 1) = 1 + \frac{(n - k + 2)(3k - n + 1)}{2},$$

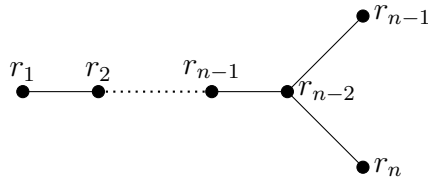
which is the rank of the action (see Lemma 6.4.2(2)). Therefore, to complete the proof it suffices to show that the sets $\Delta_{n-k,j}$ each split into at least two orbitals. To do this, we will determine the orbitals which split for the corresponding action of the Weyl group and then use the correspondence in Lemma 6.3.7 to determine the result for G .

To show the result for G it suffices to show the result for $H := \Omega_{2n}^+(q)$.

Let e_i, f_i be the standard basis ordered as follows: $e_1, \dots, e_n, f_n, \dots, f_1$. We first find a presentation of the Weyl group of H by simple reflections. The Weyl group of H is $W := N_H(T)/T$, where

$$T := \left\{ \begin{pmatrix} \lambda_1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & \lambda_n & \ddots & & \vdots \\ \vdots & & \ddots & \lambda_n^{-1} & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & \lambda_1^{-1} \end{pmatrix} : \lambda_i \in \mathbb{F}_q^* \right\}$$

(see Section 3.7.4 in [24]). We now define some elements of H . For $\sigma \in S_n$, a permutation of $\{1, \dots, n\}$, let g_σ be the element of H which maps e_1 to $\pm e_1$, e_i to $e_{i\sigma}$ for $i \neq 1$, f_1 to $\pm f_1$, and f_i to $f_{i\sigma}$ for $i \neq 1$ (the signs can be chosen so that g_σ is in H ; see Remark 6.4.6). For $i \in \{1, \dots, n\}$, let t_i be the element of H which swaps e_i and f_i and fixes all the other basis elements. Then we have that $N_H(T) = \langle T, t_i t_j, g_\sigma | i, j = 1, \dots, n, \sigma \in S_n \rangle$ and $W = N_H(T)/T \cong C_2^{n-1} : S_n$ is a subgroup of $C_2 \wr S_n$ of index 2, with generators which are the images of the elements $t_i t_j$ and g_σ . By associating the numbers $1, \dots, n$ to $\lambda_1, \dots, \lambda_n$ and the numbers $-1, \dots, -n$ to $\lambda_1^{-1}, \dots, \lambda_n^{-1}$, we see that W acts on the set $\{\pm 1, \dots, \pm n\}$. A presentation for W by simple reflections is given by the diagram



where the nodes represent generators, the products of generators corresponding to adjacent nodes have order 3, and the products of generators corresponding to non-adjacent nodes have order 2 (see Table 2.1 in [24, p. 33]).

For $i \in \{1, \dots, n-1\}$, define $r_i := (i \ i+1)$, and define $r_n := t_{n-1}t_n(n-1 \ n)$. One can check that the images of $r_1, \dots, r_n$ satisfy the above relations and generate W , and thus form a set of simple reflections. Henceforth, we will just use r_i to denote the image of r_i .

For $k \leq n-2$, one can check that $W_k = \langle r_i | i \neq k \rangle \cong S_k \times (C_2^{n-k-1} : S_{n-k})$, which is the stabiliser of the k -subset $\{1, \dots, k\}$ in the action of W on the set $I_{\pm}^{\{k\}}$ of k -subsets of $\{\pm 1, \dots, \pm n\}$ where no k -subset can include $+$ and $-$ of the same element. Moreover, the latter action can be seen to be transitive using the Orbit-Stabiliser theorem. Thus, we conclude that the action of W on $(W : W_k)$ is equivalent to the action of W on $I_{\pm}^{\{k\}}$. Now, for $j \in \{0, \dots, 2k-n\}$, define the following k -subsets of $I_{\pm}^{\{k\}}$:

$$\begin{aligned}\alpha &:= \{1, \dots, k\}, \\ \beta^+ &:= \{1, \dots, j, k+1, \dots, n, -(j+1), \dots, -(2k-n)\} \\ \beta^- &:= \{1, \dots, j, k+1, \dots, n-1, -n, -(j+1), \dots, -(2k-n)\}.\end{aligned}$$

Suppose there exists $w \in W$ such that $(\alpha, \beta^+)^w = (\alpha, \beta^-)$. Then $w \in W_k$, and must map the numbers $k+1, \dots, n$ to the numbers $k+1, \dots, n-1, -n$. However, elements of W_k can only change the sign of an even number of elements from $k+1, \dots, n$, and thus (α, β^+) and (α, β^-) must be in different orbitals of W .

Now if $W_k w_i W_k$ are the distinct suborbits of W , then by Lemma 6.3.7, $P_k w_i P_k$ are the distinct suborbits of H . So the distinct orbitals $(W_k, W_k w_i)^W$ of W correspond to the distinct orbitals $(P_k, P_k w_i)^H$ of H . Now the orbital containing (α, β^+) corresponds (under the equivalent action) to the orbital containing $(W_k, W_k w)$, where w maps α to β^+ . The orbital containing the latter corresponds (under Lemma 6.3.7) to the orbital containing $(P_k, P_k w)$ which corresponds (under the equivalent action) to the orbital containing (A, B^+) . Similarly, the orbital containing (α, β^-) corresponds to the orbital containing (A, B^-) . Now both pairs $(A, B^{\pm})$ are in $\Delta_{n-k,j}$ and thus

this proves that $\Delta_{n-k,j}$ splits into at least two orbitals of H , one containing (A, B^+) and the other containing (A, B^-) , as required. $\square$

Remark 6.4.6. Let A be the $n \times n$ permutation matrix corresponding to the permutation of $e_1, \dots, e_n$ by the element g_σ in the proof of Proposition 6.4.5. Note that $\det(A) = \pm 1$. Now, it can be shown that g_σ lies in $\Omega_{2n}^+(q)$ if and only if $\det(A) = 1$, and we can ensure the latter by choosing the appropriate signs in the definition of g_σ .

Proposition 6.4.7. *Let (G, Y) be a primitive permutation group where $G := \text{P}\Omega_{2n}^+(q)$ and $Y := (G : P_n)$, where P_n is a maximal parabolic subgroup of G . The action of G on Y is equivalent to the natural action of G on the set V_n . Let Δ_{ij} be as in Proposition 6.4.4. For n odd, the non-diagonal orbitals of (G, V_n) are $\Delta_{0,2l+1}$, where $l \in \{0, \dots, \frac{n-3}{2}\}$. For n even, the non-diagonal orbitals of (G, V_n) are $\Delta_{0,2l}$, where $l \in \{0, \dots, \frac{n-2}{2}\}$.*

Proof. The first statement in the result follows from Proposition 6.3.5. We claim that the sets $\Delta_{0,2l+1}$ (for n odd) and $\Delta_{0,2l}$ (for n even) are non-empty. Indeed, let

$$\begin{aligned} U &:= \langle e_1, \dots, e_n \rangle, \\ W_1 &:= \langle e_1, \dots, e_{2l+1}, f_{2l+2}, \dots, f_n \rangle, \\ W_2 &:= \langle e_1, \dots, e_{2l}, f_{2l+1}, \dots, f_n \rangle \end{aligned}$$

where e_i, f_i are the standard basis vectors. Then $n - \dim(U \cap W_i)$ is even where n is odd and n is even for $i = 1, 2$ respectively, and $(U, W_1) \in \Delta_{0,2l+1}$ and $(U, W_2) \in \Delta_{0,2l}$. Now suppose (A, B) and (C, D) are two distinct elements of V_n^2 which are in the same orbital. It is easy to see that $\dim(A \cap B) = \dim(C \cap D)$ and $\dim(\text{Rad}(A + B)) = \dim(\text{Rad}(C + D))$. Furthermore, by

counting, the total number of sets $\Delta_{0,j}$ plus the diagonal orbital is

$$\begin{cases} \frac{n-1}{2} + 1, & n \text{ odd} \\ \frac{n}{2} + 1, & n \text{ even.} \end{cases}$$

By Lemma 6.4.2(3), this is precisely the rank of the action and thus the non-diagonal orbitals are precisely the $\Delta_{0,j}$ described in the statement. $\square$

Note that the orbitals Δ_i in Proposition 6.4.1 and Δ_{ij} in Proposition 6.4.4 are self-paired; we will denote the corresponding orbital graphs by Γ_i and Γ_{ij} , respectively.

6.5 Proof of the main result for the simple classical groups

We now prove a sequence of individual results for the orbital graphs defined in Section 6.4.

Proposition 6.5.1. *For all $k \geq 2$, we have $\text{diam}(\Gamma_{\lfloor \frac{k}{2} \rfloor}) = 2$.*

Proof. Let A and B be two k -subspaces with $\dim(A \cap B) = j \neq \lfloor \frac{k}{2} \rfloor$. We may write $A = \langle X \rangle$ and $B = \langle Y \rangle$, where $X := \{a_1, \dots, a_k\}$, $Y := \{a_1, \dots, a_j, b_{j+1}, \dots, b_k\}$ and $b_i \notin A$ for all i . Then $d(A, B) \geq 2$. If $j = 0$, then let C be the k -subset consisting of $a_1, \dots, a_{\lfloor \frac{k}{2} \rfloor}$, $b_1, \dots, b_{\lfloor \frac{k}{2} \rfloor}$, along with $a_{\frac{k-1}{2}+1} + b_{\frac{k-1}{2}+1}$ if k is odd. Now suppose $j \geq 1$. Extend $X \cup Y$ to a basis I for the underlying vector space. If $\lfloor \frac{k}{2} \rfloor \leq k - j$, then choose a k -subset C consisting of $\lfloor \frac{k}{2} \rfloor$ elements from $X \setminus Y$, $\lfloor \frac{k}{2} \rfloor$ elements from $Y \setminus X$, and $k - 2 \lfloor \frac{k}{2} \rfloor$ elements from $I \setminus (X \cup Y)$ (note that $|I \setminus (X \cup Y)| \geq k - 2 \lfloor \frac{k}{2} \rfloor$, since $n \geq 2k \geq 3k - j - 2 \lfloor \frac{k}{2} \rfloor$). If $\lfloor \frac{k}{2} \rfloor > k - j$, then choose a k -subset C consisting of $\lfloor \frac{k}{2} \rfloor - k + j$ elements from $X \cap Y$, $k - j$ elements from $X \setminus Y$, $k - j$ elements from $Y \setminus X$, and $j - \lfloor \frac{k}{2} \rfloor$ elements from $I \setminus (X \cup Y)$ (note that

$|I \setminus (X \cup Y)| \geq j - \lfloor \frac{k}{2} \rfloor$ since $n \geq 2k - \lfloor \frac{k}{2} \rfloor$. Then $\langle C \rangle$ is a common neighbour of A and B , and hence $d(A, B) = 2$. $\square$

Proposition 6.5.2. *Let (G, V_k) be a primitive permutation group, where $G := \text{PX}_n(q)$ is a simple classical group with $X \in \{\text{Sp}, \text{SU}, \Omega^\circ, \Omega^-\}$. If the rank of (G, V_k) is strictly greater than 2, then $\text{diam}(\Gamma_{0,0}) = 2$.*

Proof. Let $(A, B) \in \Delta_{ij}$, where $(i, j) \neq (0, 0)$. Then $d(A, B) \geq 2$ and to prove the result, it suffices to construct a path of length 2 between A and B . Without loss of generality, we may suppose that

$$\begin{aligned} A &= \langle e_1, \dots, e_k \rangle, \\ B &= \langle e_1, \dots, e_j, f_{j+1}, \dots, f_{k-i}, e_{k+1}, \dots, e_{k+i} \rangle, \end{aligned}$$

where e_i, f_i are as in the standard bases. Then it is straightforward to check that C is a common neighbour of A and B , where C is given below:

$\mathbf{X} = \mathbf{Sp}$:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+1}, \dots, f_{k-i} + e_{k-i}, f_{k-i+1} + f_{k+1}, \dots, f_k + f_{k+i} \rangle.$$

Note that since the form is symplectic, all vectors are isotropic.

$\mathbf{X} = \mathbf{SU}$: Recall that a unitary form is defined over a field $\mathbb{F}_q$, where $q = q_0^2$. Pick an element $\lambda \in \mathbb{F}_{q_0}^*$ such that $\lambda + \lambda^{q_0} = 0$; note that such a λ exists since the map $\mathbb{F}_q \rightarrow \mathbb{F}_{q_0}$ given by $\mu \mapsto \mu + \mu^{q_0}$ is surjective (see Proposition 11.2.1 in [11]) and thus its kernel has q_0 elements in it. Define

$$C := \langle f_1, \dots, f_j, f_{j+1} + \lambda e_{j+1}, \dots, f_{k-i} + \lambda e_{k-i}, f_{k-i+1} + f_{k+1}, \dots, f_k + f_{k+i} \rangle.$$

Note that the vector $f_r + \lambda e_r$ is totally isotropic since $(f_r + \lambda e_r, f_r + \lambda e_r) = \lambda + \lambda^{q_0} = 0$.

$\mathbf{X} = \Omega^\circ, \Omega^-$: Let x be as in the standard basis with $Q(x) = 1$ (see Proposition 2.3.11). Pick $\lambda \in \mathbb{F}_q^*$ and define $\mu := -\lambda^2$. Define

$$C := \langle f_1, \dots, f_j, f_{j+1} + \mu e_{j+1} + \lambda x, \dots, f_{k-i} + \mu e_{k-i} + \lambda x, \\ f_{k-i+1} + f_{k+1}, \dots, f_k + f_{k+i} \rangle.$$

Note that the vector $v := f_r + \mu e_r + \lambda x$ is totally singular since $Q(v) = Q(f_r + \mu e_r) + Q(\lambda x) + (f_r + \mu e_r, \lambda x) = \mu + \lambda^2 = 0$. $\square$

Proposition 6.5.3. *Let (G, V_k) be a primitive permutation group, where $G := \text{P}\Omega_{2n}^+(q)$ and $k \leq n - 2$. Then $\text{diam}(\Gamma_{0,0}) = 2$.*

Proof. Firstly suppose $n > 2k$. Let $(A, B) \in \Delta_{ij}$, where $(i, j) \neq (0, 0)$. Then $d(A, B) \geq 2$ and to prove the result, it suffices to construct a path of length 2 between A and B . Without loss of generality, we may suppose that

$$A = \langle e_1, \dots, e_k \rangle, \\ B = \langle e_1, \dots, e_j, f_{j+1}, \dots, f_{k-i}, e_{k+1}, \dots, e_{k+i} \rangle,$$

where e_i, f_i are as in the standard bases. Then it is straightforward to check that C is a common neighbour of A and B , where C is given below:

$k - i - j$ even:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{k-i-1} + e_{k-i}, f_{k-i} - e_{k-i-1}, \\ f_{k-i+1} + f_{k+1}, \dots, f_k + f_{k+i} \rangle.$$

$k - i - j$ odd and $i = 0$:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{k-2} + e_{k-1}, f_{k-1} - e_{k-2}, \\ f_k + e_k + f_{k+1} - e_{k+1} \rangle.$$

Note that $n \geq k + 2$ and therefore the basis vectors e_{k+1} and f_{k+1} exist.

$k - i - j$ odd and $i > 0$:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{k-i-2} + e_{k-i-1}, f_{k-i-1} - e_{k-i-2}, \\ f_{k-i} + e_{k-i} + f_{k-i+1} - e_{k-i+1} + e_{k+1}, f_{k-i+1} + f_{k+1}, \dots, f_k + f_{k+i} \rangle.$$

Now suppose $n \leq 2k$. By Proposition 6.4.5 and the above, it remains to show $d(A, B) = 2$, where

$$A := \langle e_1, \dots, e_k \rangle, \\ B := \langle e_1, \dots, e_j, e_{k+1}, \dots, e_{n-1}, f_n, f_{j+1}, \dots, f_{2k-n} \rangle.$$

Indeed, C is a common neighbour of A and B , where C is given below:

$2k - n - j$ even:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{2k-n-1} + e_{2k-n}, \\ f_{2k-n} - e_{2k-n-1}, f_{2k-n+1} + f_{k+1}, \dots, f_{k-1} + f_{n-1}, f_k + e_n \rangle.$$

$2k - n - j$ odd:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{2k-n-2} + e_{2k-n-1}, \\ f_{2k-n-1} - e_{2k-n-2}, f_{2k-n} + e_{2k-n} + f_{2k-n+1} - e_{2k-n+1} + e_{k+1}, \\ f_{2k-n+1} + f_{k+1}, \dots, f_{k-1} + f_{n-1}, f_k + e_n \rangle.$$

□

Proposition 6.5.4. *Let (G, V_n) be a primitive permutation group, where $G := \text{P}\Omega_{2n}^+(q)$. Suppose that the rank of (G, V_k) is strictly greater than 2. If n is even, then $\text{diam}(\Gamma_{0,0}) = 2$, and if n is odd, then $\text{diam}(\Gamma_{0,1}) = 2$.*

Proof. Let $(A, B) \in \Delta_{0,j}$, where $j \in \{0, \dots, n-2\}$ ($j \neq 0$ even for n even and $j \neq 1$ odd for n odd). Then $d(A, B) \geq 2$ and to prove the result, it suffices to construct a path of length 2 between A and B . Without loss of generality, we may suppose that

$$\begin{aligned} A &= \langle e_1, \dots, e_n \rangle, \\ B &= \langle e_1, \dots, e_j, f_{j+1}, \dots, f_n \rangle, \end{aligned}$$

where e_i, f_i are as in the standard bases. Then it is straightforward to check that C is a common neighbour of A and B , where C is given below:

n even:

$$C := \langle f_1, \dots, f_j, f_{j+1} + e_{j+2}, f_{j+2} - e_{j+1}, \dots, f_{n-1} + e_n, f_n - e_{n-1} \rangle.$$

n odd:

$$C := \langle f_1, \dots, f_j, e_{j+1}, f_{j+2}, f_{j+3} + e_{j+4}, f_{j+4} - e_{j+3}, \dots, f_{n-1} + e_n, f_n - e_{n-1} \rangle.$$

□

We have also found other orbital graphs of diameter 2 for $(\text{P}\Omega_{2n}^+(q), V_n)$ when n is odd, as described below.

Proposition 6.5.5. *Let (G, V_n) be a primitive permutation group, where $G := \text{P}\Omega_{2n}^+(q)$ and n is odd. Suppose that the rank of (G, V_k) is strictly greater than 2. If $n \equiv 1 \pmod{4}$, then $\text{diam}(\Gamma_{0, \lceil \frac{n}{2} \rceil}) = 2$, and if $n \equiv 3 \pmod{4}$, then $\text{diam}(\Gamma_{0, \lfloor \frac{n}{2} \rfloor}) = 2$.*

Proof. Let $(A, B) \in \Delta_{0,j}$, where $j \in \{1, \dots, n-2\}$ with j odd and $j \neq \lceil \frac{n}{2} \rceil, \lfloor \frac{n}{2} \rfloor$, respectively for $n \equiv 1, 3 \pmod{4}$. Then $d(A, B) \geq 2$ and to prove the result, it suffices to construct a path of length 2 between A and B .

Without loss of generality, we may suppose that

$$\begin{aligned} A &= \langle e_1, \dots, e_n \rangle, \\ B &= \langle e_1, \dots, e_j, f_{j+1}, \dots, f_n \rangle, \end{aligned}$$

where e_i, f_i are as in the standard bases. Then it is straightforward to check that C is a common neighbour of A and B , where C is given below:

$n \equiv 1 \pmod{4}$: Note that $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$. Define

$$C := \langle e_1, \dots, e_{\frac{j+1}{2}}, e_{j+1}, \dots, e_{\frac{n+j}{2}}, f_{\frac{n+j}{2}+1}, \dots, f_n, f_{\frac{j+1}{2}+1}, \dots, f_j \rangle.$$

$n \equiv 3 \pmod{4}$: Note that $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$. Define

$$C := \langle e_1, \dots, e_{\frac{j-1}{2}}, e_{j+1}, \dots, e_{\frac{n+j}{2}}, f_{\frac{n+j}{2}+1}, \dots, f_n, f_{\frac{j-1}{2}+1}, \dots, f_j \rangle.$$

□

We now have all the ingredients needed to prove part 2 of Theorem 6.2.1. In order to prove part 1 of Theorem 6.2.1, we will need to verify the existence of an orbital graph of diameter at least 3 for the majority of the parabolic actions of the simple classical groups. For this, we shall make use of the following result, which follows from Proposition 10.6.7 in [4].

Lemma 6.5.6. *Let G be a group with a (B, N) -pair. Let W be the Weyl group of G which is generated by the simple reflections w_i . Let Γ be the orbital graph corresponding to the orbital $\Delta := (W_k, W_k w_k)^W$ of the action of W on $(W : W_k)$, and let $d := \text{diam}(\Gamma)$. The action of G on $(G : P_k)$ has an orbital graph of diameter d .*

Remark 6.5.7. Consider Lemma 6.5.6 with $G = \text{SL}_n(q)$. Then $W \cong S_n$ and is generated by the simple reflections $w_i = (i \ i+1)$ for $i \in \{1, \dots, n-1\}$

(see [24, p. 47]). Moreover, $W_k \cong S_k \times S_{n-k}$ and thus Γ is the graph $\Gamma_{n,k,k-1}$ from Chapter 3, which has diameter k .

We now state a result which gives the diameter of the graph Γ from Lemma 6.5.6 for all the classical groups; see Proposition 10.4.3 in [4].

Lemma 6.5.8. *Let (G, Y) be a primitive permutation group where G is a classical group and $Y := (G : P_k)$, where P_k is a maximal parabolic subgroup of G . Let Γ be the graph from Lemma 6.5.6 and let $d := \text{diam}(\Gamma)$. Then d is given in Table 6.2.*

G	d
$\text{SL}_n(q)$	k
$\text{Sp}_{2n}(q), \text{SU}_{2n}(q), \text{SU}_{2n+1}(q),$ $\Omega_{2n+1}(q), \Omega_{2n+2}^-(q)$	n for $k = n$ $k + 1$ for $k < n$
$\Omega_{2n}^+(q)$	$\lfloor n/2 \rfloor$ for $k = n, n - 1$ $k + 1$ for $k < n - 1$

Table 6.2: Diameter of a special orbital graph of (G, P_k)

We now give a proof of the main result.

Proof of Theorem 6.2.1. Let (G, Y) be as in the statement of the result where $G = \text{PX}_n(q)$. By Propositions 6.3.1, 6.3.4 and 6.3.5, we may assume that $Y = V_k$. Suppose $\text{diam}_O(G, Y) \leq 2$. By Lemma 6.5.6, $(X_n(q), Y)$ and thus $(\text{PX}_n(q), Y)$ has an orbital graph of diameter d where d is as in Table 6.2 from Lemma 6.5.8. Thus, we must have $d \leq 2$ which yields exactly the values of k and n as in the statement of the result. Conversely, the values of n and k in the statement of the result give rise to actions of rank equal to either 2 or 3 (the ranks can be calculated using Proposition 6.4.1 and Lemma 6.4.2), and therefore $\text{diam}_O(G, Y) \leq 2$ in these cases. This proves part 1.

The only pairs (X_n, k) for which the rank of (G, Y) is 2 are the ones in the statement of the result (see Remark 6.4.3). If (X_n, k) is not amongst this list then Propositions 6.5.1, 6.5.2, 6.5.3 and 6.5.4 assert that (G, Y) has an orbital graph of diameter 2. This proves part 2. $\square$

6.6 Proof of the main result for the exceptional groups of Lie type

To prove Theorem 6.2.5, we shall not need to explicitly define the exceptional groups of Lie type as we will only be working with the associated Weyl groups. The Weyl groups of $E_6(q)$, $E_7(q)$, $E_8(q)$, $G_2(q)$, $F_4(q)$ can be found in Section 3.12.4 in [24]. The Weyl groups of ${}^2E_6(q)$ and ${}^3D_4(q)$ are isomorphic to the Weyl groups of $F_4(q)$ and $G_2(q)$, respectively, and the Weyl group of ${}^2F_4(2^{2m+1})$ is isomorphic to D_{16} (see Section 13.3 in [5]). Recall from Definition 6.1.1 that the rank of a Weyl group is the number of simple reflections that it is generated by. The ranks of the Weyl groups of the exceptional groups mentioned above can be found in [5, p. 43,224]. We collate the above information in the following result.

Proposition 6.6.1. *The Weyl groups of the groups $E_6(q)$, $E_7(q)$, $E_8(q)$, $G_2(q)$, $F_4(q)$, ${}^2E_6(q)$, ${}^3D_4(q)$, and ${}^2F_4(2^{2m+1})$ are as follows:*

Group	Weyl group	Rank
$E_6(q)$	$\mathrm{SO}_5(3)$	6
$E_7(q)$	$C_2 \times \mathrm{Sp}_6(2)$	7
$E_8(q)$	$2.O_8^+(2)$	8
$G_2(q)$	D_{12}	2
$F_4(q)$	$O_4^+(3)$	4
${}^2E_6(q)$	$O_4^+(3)$	4
${}^3D_4(q)$	D_{12}	2
${}^2F_4(2^{2m+1})$	D_{16}	2

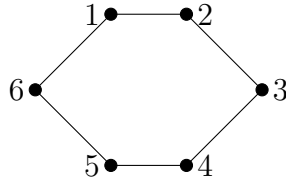
In order to prove the main result, we will need to verify the existence of an orbital graph of diameter at least 3 for the majority of the parabolic actions of the exceptional groups. For this, we shall make use of Lemma 6.5.6. Since the Weyl groups of the exceptional groups are independent of the value of q (see Proposition 6.6.1), the diameter of the orbital graph described in

Lemma 6.5.6 can be calculated using a computer, for example through the use of Magma. We now give a proof of Theorem 6.2.5.

Proof of Theorem 6.2.5. If $G = {}^2B_2(2^{2m+1})$ or $G = {}^2G_2(3^{2m+1})$, then there is only one parabolic action (see Sections 13.3.5 and 13.3.6 in [5]) which is 2-transitive (see [24, p. 117,137]) and thus there is only one orbital graph of diameter 1, which implies $\text{diam}_O(G, X) \leq 2$. If $G = E_6(q)$ and $k = 1, 6$, then the actions have rank 3 (see [24, p. 171]) and thus again we have $\text{diam}_O(G, X) \leq 2$. It remains to show that for the remaining parabolic actions there exists an orbital graph of diameter at least 3.

Firstly, suppose G is one of $E_6(q)$, $E_7(q)$, $E_8(q)$, or $F_4(q)$, and P_k is a parabolic subgroup of G , where $k \neq 1, 6$ if $G = E_6(q)$. By Lemma 6.5.6, (G, X) has an orbital graph of diameter $d := \text{diam}(\Gamma)$, where Γ is the orbital graph corresponding to the orbital $\Delta := (W_k, W_k w_k)^W$ of the action of the Weyl group W on $(W : W_k)$. Now the values for d have been computed in previous literature and can be found in Table 10.5 in [4, p. 317]. One can check that $d \geq 3$ and thus $\text{diam}_O(G, X) \geq 3$.

If $G = G_2(q)$, then by Proposition 6.6.1, the Weyl group of G is $W \cong D_{12}$, where we view D_{12} acting on the set $\{1, \dots, 6\}$ as the group of rotations and reflections of a regular hexagon labelled as follows:

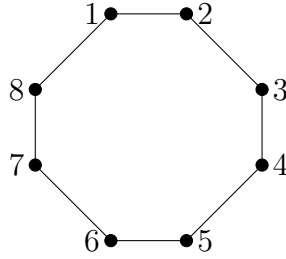


Now W is generated by the simple reflections $r_1 := (26)(35)$ and $r_2 := (16)(25)(34)$ (see [24, p. 103]). Recall that $W_i = \langle r_i \rangle$, for $i = 1, 2$. Now W acts on the vertices and edges of the hexagon. Moreover, W_1 is the stabiliser in W of the vertex 1, and W_2 is the stabiliser in W of the edge 1–6, and thus both actions are transitive by the Orbit-Stabiliser property. We conclude that the action of W on $(W : W_i)$ is equivalent to the action of W on the vertices

and edges of the hexagon, respectively for $i = 1, 2$. It is straightforward to work out the orbital graphs of the latter two actions. We find that each action has two disconnected orbital graphs and one connected orbital graph of diameter 3. Thus the graph Γ from Lemma 6.5.6 has diameter 3, and hence (G, X) must also have an orbital graph of diameter 3, i.e. $\text{diam}_O(G, X) \geq 3$.

If $G = {}^2E_6(q)$ or ${}^3D_4(q)$, then by Proposition 6.6.1, the Weyl group of G is isomorphic to the Weyl group of $F_4(q)$ and $G_2(q)$, respectively, and thus as in the preceding paragraphs, we have $\text{diam}_O(G, X) \geq 3$.

Now suppose $G = {}^2F_4(2^{2m+1})$. By Proposition 6.6.1, the Weyl group of G is $W \cong D_{16}$, where we view D_{16} acting on the set $\{1, \dots, 8\}$ as the group of rotations and reflections of a regular octagon labelled as follows:



Now W is generated by the simple reflections $r_1 =: (28)(37)(46)$ and $r_2 := (12)(38)(47)(56)$ (see Section 13.3.7 in [5]). Recall that $W_i = \langle r_i \rangle$, for $i = 1, 2$. Now W acts on the vertices and edges of the octagon. Moreover, W_1 is the stabiliser in W of the vertex 1, and W_2 is the stabiliser in W of the edge $1 - 2$, and thus both actions are transitive by the Orbit-Stabiliser property. We conclude that the action of W on $(W : W_i)$ is equivalent to the action of W on the vertices and edges of the octagon, respectively for $i = 1, 2$. It is straightforward to work out the orbitals and orbital graphs of the latter two actions. We find that each action has two disconnected orbital graphs and two connected orbital graphs of diameter 4. Thus the graph Γ from Lemma 6.5.6 must have diameter 4, and hence (G, X) must also have an orbital graph of diameter 4. This concludes the proof. $\square$

Chapter 7

Open problems

In this chapter we discuss some open problems which arise from the work in the thesis. As mentioned in the introduction, one broad aim would be to find an explicit list of all almost simple finite primitive permutation groups whose orbital diameters are at most d for small values of d , say $d = 2, 3, 4, 5$. For the almost simple groups with socle an alternating group A_n ($n \neq 6$), we have established the result for $d = 5$ in Chapter 3. One could aim to prove a similar result for values higher than 5.

Problem 7.1. *Find the primitive groups (G, X) with $\text{diam}_O(G, X) \leq d$ for $d \leq 10$, where $G := S_n$ or A_n .*

To solve Problem 7.1, it may be helpful to use the result proposed in Conjecture 3.4.6.

Problem 7.2. *Prove Conjecture 3.4.6.*

For the action of the alternating group A_{k^2} on the set $X := I^{(k,k)}$ of (k, k) -partitions of $\{1, \dots, k^2\}$, we showed that if k is odd or k is even and $k/2$ is odd, then (G, X) has an orbital graph of diameter 2. One could investigate the existence of orbital graphs of diameter 2 for the remaining case.

Problem 7.3. *Prove or disprove the existence of an orbital graph of diameter 2 for (G, X) , where $G := A_{k^2}$ and $X := I^{(k,k)}$ with k even and $k/2$ even.*

One could also investigate the existence of orbital graphs of diameter 2 for the general case of the actions of S_n and A_n on $I^{(k,l)}$, where $n = kl$.

Problem 7.4. *Prove or disprove the existence of an orbital graph of diameter 2 for (G, X) , where $G := S_{kl}$ or A_{kl} and $X := I^{(k,l)}$.*

The following problems arise from the work done on the groups $\text{PSL}_2(q)$ in Chapter 4.

Problem 7.5. *Prove or disprove the converse for the group $\text{PSL}_2(q^{1/3})$ in Theorem 4.2.1(1).*

Problem 7.6. *Prove or disprove the existence of an orbital graph of diameter 2 for (G, X) where $G := \text{PSL}_2(q)$ and $X := (G : H)$, with $H \cong D_{q-1}$ and $q \equiv 1 \pmod{4}$, or with $H \cong \text{PGL}_2(q^{1/2})$ and $q^{1/2} \equiv 1 \pmod{4}$ (see Conjecture 4.4.2).*

Problem 7.7. *Prove Conjectures 4.3.3 and 4.3.41.*

The following is a general problem one could aim to tackle.

Problem 7.8. *Determine results similar to Theorems 6.2.1 and 6.2.5 for all primitive actions of the simple groups of Lie type.*

Bibliography

- [1] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, second edition, 2000.
- [2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [3] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013.
- [4] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Results in Mathematics and Related Areas (3)*. Springer-Verlag, Berlin, 1989.
- [5] Roger W. Carter. *Simple groups of Lie type*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.
- [6] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

- [7] Yongzhu Chen and Weifan Wang. Diameters of uniform subset graphs. *Discrete Math.*, 308(24):6645–6649, 2008.
- [8] Yongzhu Chen and Yingqian Wang. On the diameter of generalized Kneser graphs. *Discrete Math.*, 308(18):4276–4279, 2008.
- [9] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
- [10] Graham Everest and Thomas Ward. *An introduction to number theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2005.
- [11] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [12] Dieter Jungnickel. *Graphs, networks and algorithms*, volume 5 of *Algorithms and Computation in Mathematics*. Springer, Berlin, third edition, 2008.
- [13] Ireri Nthiga Kamuti. *Combinatorial formulas, invariants and structures associated with primitive permutation representations of $PSL(2, q)$ and $PGL(2, q)$* . PhD thesis, University of Southampton, United Kingdom, 1992.
- [14] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.
- [15] Martin W. Liebeck, Dugald Macpherson, and Katrin Tent. Primitive permutation groups of bounded orbital diameter. *Proc. Lond. Math. Soc. (3)*, 100(1):216–248, 2010.

- [16] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra*, 111(2):365–383, 1987.
- [17] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On the O’Nan–Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44(3):389–396, 1988.
- [18] Attila Maróti. On the orders of primitive groups. *J. Algebra*, 258(2):631–640, 2002.
- [19] Cheryl E. Praeger and Leonard H. Soicher. *Low rank representations and graphs for sporadic groups*, volume 8 of *Australian Mathematical Society Lecture Series*. Cambridge University Press, Cambridge, 1997.
- [20] J.P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics. Springer New York, 1973.
- [21] Atiqah Sheikh. Orbital diameters of the symmetric and alternating groups. *J. Algebraic Combin.*, 45(1):1–32, 2017.
- [22] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [23] Donald E. Taylor. *The geometry of the classical groups*, volume 9 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1992.
- [24] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

Appendix A

Number theoretical methods

In this chapter we prove all the number theoretical arguments which have been used in Sections 4.3 and 4.4 of Chapter 4.

Lemma A.1. *Let $a \in \mathbb{F}_q \setminus \{\pm 1\}$. Let n be the number of solutions $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ to the equation*

$$(x^2 - 1)(x^2 - a^2) = y^2. \quad (\text{A.1})$$

If $q \geq 17$, then $n \geq 1$.

In order to prove Lemma A.1 we will need the following theory regarding *elliptic curves*. For more details on the topic, one can see Chapter 3 in [22].

Definition A.2. A curve of the form

$$C : y^2 = f(x) := x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{F}_q$ is called an *elliptic curve* over $\mathbb{F}_q$ if the *discriminant* $\Delta_f := a^2b^2 - 4b^3 - 4a^3c - 27c^2$ of f is non-zero.

Theorem A.3 (Hasse's Theorem, [6, p. 118]). *Let C be an elliptic curve over $\mathbb{F}_q$. The number N of points of C defined over $\mathbb{F}_q$ (including the 'point at infinity') satisfies*

$$|N - (q + 1)| \leq 2q^{1/2}.$$

Remark A.4. The 'point at infinity' referred to in Hasse's Theorem is a 'point' which satisfies the 'projective' version of the elliptic curve in question, but does not translate to a point which satisfies the original elliptic curve.

Proof of Lemma A.1. Assume $q \geq 17$. Suppose first that $a = 0$. The number of solutions (c, d) over $\mathbb{F}_q$ to the equation $c^2 - d^2 = 1$ where both c and d are non-zero is at least $q - 5$ (see Lemma A.8). Since $q > 5$ we can pick such a solution (c, d) . Then $(x, y) = (c, cd)$ is a solution to (A.1). Now suppose $a \neq 0$. Define

$$t := y + \left(x^2 - \frac{1 + a^2}{2} \right) \tag{A.2}$$

$$s := xt = xy + x^3 - \frac{x(1 + a^2)}{2}. \tag{A.3}$$

It can be checked that (s, t) satisfy the equation

$$2s^2 - (1 + a^2)t^2 - t^3 - \left(\frac{1 - a^2}{2} \right)^2 t = 0. \tag{A.4}$$

Now we claim that there is a bijection between solutions (x, y) of (A.1) and solutions $(s, t) \neq (0, 0)$ of (A.4). Indeed, if (x, y) is a solution of (A.1) then s and t as in (A.3) and (A.2) satisfy (A.4). Note that if $(s, t) = (0, 0)$, then $y = \frac{1+a^2}{2} - x^2$, and substituting this into (A.1) implies that $a = \pm 1$ which is not possible by assumption. Hence $(s, t) \neq (0, 0)$. Conversely, if $(s, t) \neq (0, 0)$ is a solution of (A.4), then let

$$x = \frac{s}{t}, \quad y = t - \left(\frac{s}{t} \right)^2 + \frac{1 + a^2}{2}.$$

It can be checked that (x, y) is a solution of (A.1). This proves the claim. In order to use Hasse's Theorem we need to verify that (A.4) is an elliptic curve. Rearrange (A.4) to get $(4s)^2 = f(t)$, where

$$f(t) := (2t)^3 + 2(1 + a^2)(2t)^2 + (1 - a^2)^2(2t).$$

Now (A.4) is an elliptic curve if and only if $\Delta_f \neq 0$. It can be checked that this is if and only if $a \neq 0, \pm 1$. Therefore (A.4) is an elliptic curve and now by Hasse's Theorem, if N is the number of solutions to (A.4) (including the point at infinity), then

$$|N - 1 - q| \leq 2q^{1/2}.$$

In particular, $N \geq q + 1 - 2q^{1/2} = (q^{1/2} - 1)^2$. Now the point at infinity and $(s, t) = (0, 0)$ do not translate to give solutions of (A.1). So (A.1) has at least $(q^{1/2} - 1)^2 - 2$ solutions, including points (x, y) with $x = 0$ or $y = 0$. Substituting $x = 0$ and $y = 0$ into (A.1) we see that there are only 6 such points. Therefore we conclude that

$$n \geq (q^{1/2} - 1)^2 - 8.$$

Finally, since $q \geq 17$, we have that $n \geq 1.7 \geq 1$. □

Lemma A.5. *Let $q \geq 17$ (resp. $q \geq 19$) and $\lambda \neq 0, \pm 1$. There exists $u \in \mathbb{F}_q$ such that $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ and $(1 - \lambda^2)u^2 - \lambda^2$ is a square (resp. non-square).*

Proof. Define $y := 1 - \lambda^2$ and $f(u) := yu^2 + y - 1$, and let Q denote the set of squares in $\mathbb{F}_q$. Then $y \neq 0, 1$. Suppose $y \in Q$. We have

$$\{f(u) : u \in \mathbb{F}_q\} = \{a^2 + x : a \in \mathbb{F}_q\},$$

where $x := y - 1 \neq 0$, and we also have

$$S := \{u \in \mathbb{F}_q : f(u) \in Q\} = \{a \in \mathbb{F}_q : \exists b \in \mathbb{F}_q, b^2 - a^2 = x\}.$$

Now the number of solutions (a, b) to $b^2 - a^2 = x$ is $q - 1$ (see Lemma A.8). If $b = 0$ is a solution, then

$$|S| = \frac{q - 1 - 2}{2} + 2 = \frac{q + 1}{2},$$

and otherwise $|S| = \frac{q-1}{2}$. Hence, the number of values of u for which $f(u)$ is non-square is at least

$$q - \frac{q + 1}{2} = \frac{q - 1}{2}.$$

Now the number of solutions u to $u^2 = -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ is at most 7. Since $q \geq 17$, we have $\frac{q+1}{2} - 7 \geq \frac{q-1}{2} - 7 \geq 1$, and therefore there is at least one value of u with $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ for which $f(u)$ is a square, and another for which $f(u)$ is a non-square. Now suppose $y \notin Q$ and let NQ denote the set of non-squares in $\mathbb{F}_q$. We have

$$NS := \{u \in \mathbb{F}_q : f(u) \in NQ\} = \{a \in \mathbb{F}_q : \exists b \in \mathbb{F}_q^* : b^2 - a^2 = x\},$$

where now $x := \frac{y-1}{y}$. As before, the number of solutions (a, b) to $b^2 - a^2 = x$ is $q - 1$. If $b = 0$ is a solution, then

$$|NS| = \frac{q - 1 - 2}{2} = \frac{q - 3}{2},$$

and otherwise $|NS| = \frac{q-1}{2}$. Hence, the number of values of u for which $f(u)$ is square is at least

$$q - \frac{q - 1}{2} = \frac{q + 1}{2}.$$

Now for $q \geq 17$, we have $\frac{q+1}{2} - 7 \geq 1$ and for $q \geq 19$, we have $\frac{q-3}{2} - 7 \geq 1$. Thus, there is at least one value of u with $u^2 \neq -1, 0, \frac{\pm(1-\lambda)}{1+\lambda}$ for which $f(u)$ is a square, and another for which $f(u)$ is a non-square. $\square$

Lemma A.6. *Let q be an odd prime power. Then $-1 \in \mathbb{F}_q$ is a square if and only if $q \equiv 1 \pmod{4}$.*

Proof. Firstly, we claim that $-1 \in \mathbb{F}_q$ is a square if and only if $\mathbb{F}_q^*$ contains an element of order 4. Indeed, suppose $-1 \in \mathbb{F}_q$ is a square, i.e. $-1 = x^2$. Then $x^4 = 1$ and the order of x must divide 4. However, the order cannot be 1 or 2 and thus must be 4. Conversely, suppose $\mathbb{F}_q^*$ contains an element of order 4, say $y^4 = 1$. Then $y^2 = \pm 1$. However, $y^2 \neq 1$ since the order of y is 4, and thus $y^2 = -1$, i.e. -1 is a square. This proves the claim. Now it is well-known that $\mathbb{F}_q^* \cong C_{q-1}$ (see Theorem 2 in [20]), and that C_{q-1} contains an element of order 4 if and only if 4 divides $q-1$, i.e. $q \equiv 1 \pmod{4}$. This completes the proof. $\square$

Lemma A.7. *Let q be an odd prime power. The number of solutions $(x, y) \in (\mathbb{F}_q)^2$ to the equation $x^2 + y^2 = 1$ is $q + 1$ if $q \equiv 3 \pmod{4}$ and $q - 1$ if $q \equiv 1 \pmod{4}$.*

Proof. One solution is $(1, 0)$. Suppose $(x, y) \neq (1, 0)$ is a solution and define $v := \frac{y}{x-1}$. Then

$$(x, y) = (1, 0) + (x-1)(1, v).$$

Now letting $t := x-1 \neq 0$ and using $x^2 + y^2 = 1$ implies $t(t(v^2 + 1) + 2) = 0$. Rearranging for t we obtain $t = \frac{-2}{v^2 + 1}$, where $v^2 + 1 \neq 0$. Hence

$$(x, y) = (1, 0) + \frac{-2}{v^2 + 1}(1, v).$$

Conversely, one can easily check that (x, y) as above satisfy $x^2 + y^2 = 1$. Thus the number of solutions to $x^2 + y^2 = 1$ is one more than the number of $v \in \mathbb{F}_q$ with $v^2 + 1 \neq 0$. Now by Lemma A.6, the equation $v^2 + 1 = 0$ has 0 solutions if $q \equiv 3 \pmod{4}$ and 2 otherwise. The proof follows. $\square$

Lemma A.8. *Let q be an odd prime power. The number of solutions $(x, y) \in (\mathbb{F}_q)^2$ to the equation $x^2 - y^2 = 1$ is $q - 1$.*

Proof. Suppose (x, y) is a solution. Then $x^2 - y^2 = (x - y)(x + y) = 1$. Define $r := x + y \neq 0$. Then $x - y = \frac{1}{r}$ and rearranging for x and y we obtain

$x = \frac{1}{2}(r + \frac{1}{r})$ and $y = \frac{1}{2}(r - \frac{1}{r})$. Hence the number of solutions (x, y) is the number of $r \in \mathbb{F}_q^*$, which is $q - 1$. $\square$

Lemma A.9. *Let q be an odd prime power. Every element $x \in \mathbb{F}_q$ can be expressed as a sum and difference of two squares.*

Proof. Consider the set $S := \{x \mp b^2 : b \in \mathbb{F}_q\}$ ($-$, $+$ to prove the result for sum and difference, respectively). Since $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$, there are $\frac{q-1}{2}$ squares in $\mathbb{F}_q^*$ and the rest are non-squares. Since 0 is also a square, we have $|S| = \frac{q+1}{2}$. Now since $\mathbb{F}_q$ only has $\frac{q-1}{2}$ non-squares, S must contain a square, say a^2 , and so there exists b such that $x = a^2 \pm b^2$. $\square$

Lemma A.10. *Let q be an odd prime power and let $\gamma \in \mathbb{F}_q$ be a non-square. Then the number of solutions $(a, b) \in (\mathbb{F}_q)^2$ to the equation $b^2 - a^2\gamma = \gamma$ is $q + 1$.*

Proof. Firstly suppose that $q \equiv 3 \pmod{4}$. Then $-1 = \gamma^{-1}v^2$ for some $v \in \mathbb{F}_q$, and the equation becomes $b^2 + v^2a^2 = \gamma$. Now the number of solutions to the latter equation is the same as the number of solutions to the equation $x^2 + y^2 = -1$. By Lemma A.9, the equation $x^2 + y^2 = -1$ has at least one solution (x_0, y_0) ; let (x, y) be another solution. If $(x, y) \neq (x_0, -y_0)$, then the equation of the line joining (x, y) and (x_0, y_0) is $y - y_0 = t(x - x_0)$, where $t \in \mathbb{F}_q$ is the slope. Now substituting $y = t(x - x_0) + y_0$ into the equation $x^2 + y^2 = -1$ gives

$$(t^2 + 1)x^2 + (2ty_0 - 2t^2x_0)x + (t^2x_0^2 - 2tx_0y_0 + y_0^2 + 1) = 0.$$

One solution to the above equation is $x = x_0$ and since the sum of the two solutions is $\frac{2t^2x_0 - 2ty_0}{t^2 + 1}$ (note that $t^2 + 1 \neq 0$ since $q \equiv 3 \pmod{4}$), the other solution is $x = x(t) = \frac{2t^2x_0 - 2ty_0}{t^2 + 1} - x_0$. Thus $y = y(t) = t(x(t) - x_0) + y_0$. This proves that every solution of $x^2 + y^2 = -1$ is either $(x_0, -y_0)$ or $(x(t), y(t))$ for some $t \in \mathbb{F}_q$. Conversely, a line with slope $t \in \mathbb{F}_q$ which passes through (x_0, y_0) intersects the curve $x^2 + y^2 = -1$ in either 1 or 2 points; 1 in the

case where the line is a tangent to the curve at (x_0, y_0) , and 2 otherwise. In the latter case the second point is given by $(x(t), y(t))$ as above. Thus the solutions of $x^2 + y^2 = -1$ are given by $(x(t), y(t))$, where $t \in \mathbb{F}_q$, and $(x_0, -y_0)$. We conclude that there are $q + 1$ solutions in total.

Now suppose $q \equiv 1 \pmod{4}$. Then $-1 = v^2$ for some $v \in \mathbb{F}_q$, and the equation becomes $\gamma y^2 + v^2 x^2 = 1$. Following the proof of Lemma A.7, the number of solutions to this equation can be shown to be $q + 1$. $\square$

Lemma A.11. *Let q be an odd prime power, $\gamma \in \mathbb{F}_q$ be a non-square and $z \in \mathbb{F}_q^*$. Then the equation $b^2 - d^2\gamma = z$ has at least one solution (b, d) with $d \neq 0$.*

Proof. First suppose that $q \equiv 3 \pmod{4}$. Then -1 is a non-square in $\mathbb{F}_q$ and so the equation becomes $b^2 + y^2 = z$, where $y^2 := -d^2\gamma$. Now if z is a square, then we may pick $d \neq 0$ such that $y^2 = z$, and so $(0, d)$ is a solution to the original equation with $d \neq 0$. If z is a non-square, then $b^2 + y^2 = z$ has a solution (b, y) by Lemma A.9 (see below), where without loss of generality $y \neq 0$ (else z is a square). Thus the original equation has a solution (b, d) with $d \neq 0$. Now suppose that $q \equiv 1 \pmod{4}$. Then -1 is a square in $\mathbb{F}_q$ and so the equation becomes $b^2 + y^2\gamma = z$, where $y^2 := -d^2$. If z is a non-square, then we may pick $d \neq 0$ such that $y^2\gamma = z$, and so $(0, d)$ is a solution to the original equation with $d \neq 0$. Suppose now that z is a square; say $z = a^2$. Using similar arguments as in the proof of Lemma A.7, one can show that the solutions (b, y) to $b^2 + y^2\gamma = z$ are $(a, 0)$ and

$$(b, y) = (a, 0) - \frac{2a}{1 + v^2\gamma}(1, v),$$

where $v \in \mathbb{F}_q$. Thus there are two solutions (b, d) of the original equation with $d = 0$ and so $q + 1 - 2 \geq 1$ solutions with $d \neq 0$. $\square$

Lemma A.12. *Let $q \geq 7$ be an odd prime power. Every non-zero element $x \in \mathbb{F}_q$ can be expressed as a sum of two non-squares.*

Proof. Let $c \in \mathbb{F}_q$ be a primitive element. Then multiplication by c takes a square to a non-square and vice versa. Suppose first that x is a square. Then $c^{-1}x$ is a non-square. By Lemma A.9, there exist $a, b \neq 0$, such that $c^{-1}x = a^2 + b^2$ and thus $x = ca^2 + cb^2$, a sum of two non-squares. Now suppose x is a non-square. Then we can write $x = cy^2$ for some y . Now the equation $y^2 = a^2 + b^2$ has at least $q - 1$ solutions by Lemma A.7. At most four of these have $a = 0$ or $b = 0$ and thus since $q > 5$, there exist $a, b \neq 0$ such that $y^2 = a^2 + b^2$, which implies $x = cy^2 = ca^2 + cb^2$, a sum of two non-squares. $\square$