BASE SIZE AND GENERATING GRAPHS OF PRIMITIVE PERMUTATION GROUPS

Veronica Kelsey

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews

2022

Base size and generating graphs of primitive permutation groups

Veronica Kelsey

University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of
Doctor of Philosophy (PhD)
at the University of St Andrews
September 2021

Declarations

Candidate's declaration

I, Veronica Kelsey, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 55000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

I was admitted as a research student at the University of St Andrews in September 2018.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 09/02/22 Signature of candidate

Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date 09/02/22 Signature of supervisor

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Veronica Kelsey, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed Copy
No embargo on print copy.

Electronic copy
No embargo on electronic copy.

Date 09/02/22 Signature of candidate

Date 09/02/22 Signature of supervisor

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Veronica Kelsey, hereby certify that no requirements to deposit original research data or digital outputs apply to this thesis and that, where appropriate, secondary data used have been referenced in the full text of my thesis.

Date 09/02/22 Signature of candidate

Acknowledgements

I would like to thank my supervisors Prof Colva Roney-Dougal and Dr Martyn Quick, for suggesting interesting problems for us to work on, for all they have taught me about writing mathematics, and for helping me during my periods of worry and self-doubt.

I am very grateful for the corrections and suggested improvements made by Prof Ruškuc and Prof Liebeck as part of my viva.

I am immensely thankful for my friends, both in St Andrews and further afield, who provided much needed distractions from work - in particular Ashley, Chiara, Jazz, Raad and Zac.

I am forever indebted to my family for supporting me through the highs and lows of research, for showing interest and feigning understanding in my incomprehensible descriptions of my work, and for reminding me that there is more to life than maths. My parents - Kelsie and Rob; my siblings - Aidan, Marian, Esther, Agnes and Dorothy; and my partner - Peter.

Funding

This work was supported by the University of St Andrews (School of Mathematics & Statistics).

Abstract

In this thesis we consider base size and properties of the generating graph for finite groups.

Let $\Omega = \{1, \ldots, n\}$, let $\mathrm{S}_n = \mathrm{Sym}(\{1, \ldots, n\})$ and let $G \leq \mathrm{S}_n$. A *base* for G is a sequence $\Lambda = (\omega_1, \ldots, \omega_k)$ of points in Ω such that the pointwise stabilizer, $G_{\omega_1,\ldots,\omega_k}$, is the identity. The *base size* of G, denoted by $\mathrm{b}(G, \Omega)$ or $\mathrm{b}(G)$, is the length of the shortest base. We say that Λ is an irredundant base if

$$G > G_{\omega_1} > G_{\omega_1,\omega_2} > \cdots > G_{\omega_1,\omega_2,\ldots,\omega_k} = 1.$$

If no irredundant base is longer than Λ, then we say that Λ is a *maximal irredundant* base for G and denote its length by $\mathrm{I}(G)$. A group is called *large base* if it is either a product action or almost simple group, and its socle is one or more copies of the alternating group A_r acting on k-sets.

Let G be a primitive subgroup of S_n that is not large base. We prove that any irredundant base for G has size at most $5 \log_2 n$. This bound is best possible up to a small multiplicative constant and is the first logarithmic bound on the size of an irredundant base for such groups. We show that for any constant c, there are infinitely many primitive groups with maximal irredundant base size at least c times the minimal base size. As a corollary of the first result, the relational complexity of G, denoted $\mathrm{RC}(G)$ (see Definition 2.2.10), is at most $5 \log_2 n + 1$. In addition the maximal size of a minimal base and the height, denoted $\mathrm{B}(G)$ and $\mathrm{H}(G)$ (see Definitions 2.2.1 and 2.2.5), are both at most $5 \log_2 n$. Furthermore, we deduce that a base for G of size at most $5 \log_2 n$ can be computed in polynomial time.

The *generating graph* $\Gamma(G)$ of a finite group G has vertex set the non-identity elements of G, with two elements connected exactly when they generate G. A *coclique* in a graph is an empty induced subgraph, so a coclique in $\Gamma(G)$ is a subset of G such that no pair of elements generate G. A coclique is maximal if it is contained in no larger coclique. It is easy to see that the non-identity elements of a maximal subgroup of G form a coclique in $\Gamma(G)$, but this coclique need not be maximal.

Let $G = \mathrm{S}_n$ or A_n. We first determine when the intransitive maximal subgroups of G are maximal cocliques in $\Gamma(G)$, and when they are not we find the unique maximal coclique in which they are contained. We then show that for sufficiently large n, the imprimitive maximal subgroups of G are all maximal cocliques in $\Gamma(G)$.

In addition, using the result on intransitive maximal subgroups we prove that a conjecture of Cameron, Lucchini, and Roney-Dougal holds for G under certain restrictions on n. Namely we prove that two elements of G have identical sets of neighbours in $\Gamma(G)$ if and only if they belong to exactly the same maximal subgroups. Finally under another set of restrictions on n we then determine precisely which maximal subgroups are maximal cocliques in $\Gamma(G)$.

Contents

Notation

Group theoretic notation

Let Ω be a finite set, let $H \leq G \leq \mathrm{Sym}(\Omega)$ and let K be a finite group. Let $g \in G$, let Λ be a sequence of distinct points of Ω, let $\Delta \subseteq \Omega$ and let $\lambda_1, \ldots, \lambda_i \in \Omega$.

$\mathrm{Dih}(2n)$	Dihedral group of order 2n
C_n	Cyclic group of order n
$\mathrm{Aut}(G)$	Automorphism group of G
$\mathrm{soc}(G)$	Socle of G
$\mathrm{N}_G(H)$	Normalizer of H in G
$C_G(H)$	Centraliser of H in G
$\mathrm{Z}(G)$	Centre of G
$G \,\mathrm{wr}\, K$	Wreath product of G and K
$\mathrm{Syl}_p(G)$	The set of Sylow p-subgroups of G for p a prime dividing the order of G
$\Phi(G)$	Frattini subgroup of G
$m(G)$	Minimal index of proper subgroup of G
$G \rtimes K$	Semidirect product of G and K
$[G : H]$	Index of H in G
$\Gamma(G)$	Generating graph of G
1 or id	The identity element
$\mathrm{Supp}(g)$	Support of g
$\mathrm{Fix}(g)$	Fixed points of g
$\Lambda\backslash\{\lambda\}$	The subsequence of Λ given by omitting λ_i
$\mathrm{Stab}_G(\Delta)$	Stabilizer of Δ in G
Δ^G	The orbit of Δ under G
G_Λ	The elements of G which fix the points of Λ pointwise
G_Δ	The elements of G which fix Δ setwise
$G_{(\Delta)}$	The elements of G which fix Δ pointwise
$G_{\lambda_1,\ldots,\lambda_i}$	The elements of G which fix $\{\lambda_1, \ldots, \lambda_i\}$ pointwise

Vector Spaces and Matrices

Let $\mathbb{F}$ be a field, let $V = \mathbb{F}^d$ a vector space of dimension d over $\mathbb{F}$, let U and W be subspaces of V.

$\mathrm{GF}(q)$	Galois field of size q
$\mathbb{F}^*$	The non-zero elements of $\mathbb{F}$
$\mathcal{PG}_m(V)$	Set of all m-dimensional subspaces of V
$\dim(U)$	Dimension of U over $\mathbb{F}$
$U \oplus W$	Direct sum of U and W
$\Omega_m^{\oplus}$, $\Omega_m^{<}$	Definition 2.7.7
$\mathrm{Supp}_x W$	The set of vectors of W with non-zero entry in the x^{th} position
$\mathbb{M}_{n,m}(\mathbb{F})$	The set of $n \times m$ matrices over a field $\mathbb{F}$
I	The identity of $\mathbb{M}_{d,d}(\mathbb{F})$
$E_{x,y}$	The element of $\mathbb{M}_{d,d}(\mathbb{F})$ with 1 in the $(x,y)^{th}$ entry and 0 elsewhere
$T(x,y)$	The matrix $I + E_{x,y}$
ι	Inverse transpose map
$\mathrm{AGL}_1(p)$	1-dimensional affine group over $\mathrm{GF}(q)$

Classical Groups

Let q be a prime power and let $d \geq 2$.

n.d.	Non-degenerate
n.s.	Non-singular
t.i.	Totally isotropic
t.s.	Totally singular
$\mathrm{PSO}_n^{\epsilon}(q)$	Projective special orthogonal group of dimension n over $\mathrm{GF}(q)$ of type ϵ
$\mathrm{P}\Omega_d^{\epsilon}$	Simple subgroup of index 2 in $\mathrm{PSO}_n^{\epsilon}(q)$
$\mathrm{PSL}_d(q)$	Projective special linear group of dimension d over $\mathrm{GF}(q)$
$\mathrm{PSp}_d(q)$	Projective symplectic group of dimension d over $\mathrm{GF}(q)$
$\mathrm{PSU}_d(q)$	Projective special unitary group of dimension d over $\mathrm{GF}(q)^2$

Numerical invariants

Let Ω be a finite set and let $G \leq \mathrm{Sym}(\Omega)$.

$\mathrm{b}(G,\Omega)$	Base size for G with respect to its action on Ω
$\mathrm{B}(G,\Omega)$	Maximal size of a minimal base for G
$\mathrm{H}(G,\Omega)$	Height of G
$\mathrm{I}(G,\Omega)$	Maximal size of an irredundant base for G
$\mathrm{RC}(G,\Omega)$	Relational complexity of G
$\ell(G)$	Maximum length of a chain of subgroups in G
$\mu(G)$	The minimal degree of G

Symmetric groups

Let $n \in \mathbb{N}$, let $H, M \leq \mathrm{Sym}(\{1, \ldots, n\})$ with H transitive and M imprimitive maximal, and let $y \in \mathrm{Sym}(\{1, \ldots, n\})$ with disjoint cycle decomposition $c_1 \cdots c_t$.

A_n	$\mathrm{Alt}(n)$ acting on $\{1, \ldots, n\}$
S_n	$\mathrm{Sym}(n)$ acting on $\{1, \ldots, n\}$
$l(c_i)$	Length of the cycle c_i
Θ_i	The support of the cycle c_i
$\mathcal{C}(y)$	Cycle type of y, $l(c_1) \cdot l(c_2) \cdot \cdots \cdot l(c_t)$
$\mathcal{C}_M(y)$	Notation 5.2.6
$\mathcal{J}_t$	The set of elements of S_n which are a product of two transpositions
$\mathcal{J}_c$	The set of cycles of S_n
$\mathcal{J}_s$	The set of elements of S_n with support size at most $2(\sqrt{n} - 1)$
$\mathcal{J}_w$	The set of Wielandt elements of S_n, Definition 4.3.2
$\mathcal{J}$	$\mathcal{J}_t \cup \mathcal{J}_c \cup \mathcal{J}_s \cup \mathcal{J}_w \subseteq \mathrm{S}_n$
$\mathcal{H}$	A block system for H
$\mathcal{M}$	The maximal system of imprimitivity for M
$y^{\mathcal{H}}$	The induced action of y on the blocks of $\mathcal{H}$
$\hat{M}$	Definition 6.2.2
Ω_i	Notation 4.1.3

Number Theory

Let $\mathbb{N}$ be the set of positive integers, let $n, k \in \mathbb{N}$, let g be a function from $\mathbb{N}$ to $\mathbb{N}$

$\lfloor k \rfloor$	Floor of k
$\lceil k \rceil$	Ceiling of k
p_k	A Bertrand prime, any prime with $\frac{k}{2} < p_k < k - 1$
$\pi(k)$	The Prime-Counting Function, the number of primes less than or equal to k
δ_{ij}	Kronecker-Delta
$\log k$	Logarithm base 2 of k
$\ln k$	Logarithm base e of k, the natural log
$\gcd(n, k)$	Greatest common divisor of n and k
$O(g)$	"Big O notation" describing the limiting behaviour of g

Chapter 1

Introduction

The first half of this thesis is devoted to the study of numerical invariants of permutation groups, sometimes called group statistics. One of the most studied numerical invariants is base size. For $G \leq \mathrm{Sym}(\Omega)$, a *base* is a sequence $(\omega_1, \ldots, \omega_k)$ of points of Ω such that $G_{\omega_1,\ldots,\omega_k} = 1$. The *base size* for G, denoted $\mathrm{b}(G, \Omega)$ or $\mathrm{b}(G)$, is the length of a shortest base. It is easily seen that two elements of G are equal exactly when they have the same action on the base points. Hence elements of G can be stored in terms of their action on points of the base, rather than on all of Ω. When $\mathrm{b}(G, \Omega)$ is significantly smaller than $|\Omega|$ this results in a computational saving.

In [38], Liebeck proved that with the exception of one family of groups, if G is a primitive subgroup of $\mathrm{S}_n := \mathrm{Sym}(\{1, \ldots, n\})$, then $\mathrm{b}(G) < 9 \log n$. This exceptional family of groups are called *large-base* groups. Here and throughout all logs are of base 2. Following in the steps of Liebeck, one area of interest is to prove similar results for other numerical invariants. For G a primitive subgroup of S_n which is not large base, we show that the size of a maximal irredundant base, denoted by $\mathrm{I}(G)$, is at most $5 \log n$. This is the first logarithmic bound for this family of groups and is best possible up to a multiplicative constant. We also prove that for any constant c, there are infinitely many examples of primitive groups with $\mathrm{I}(G) > c\mathrm{b}(G)$. It will follow as a corollary of our upper bound on $\mathrm{I}(G)$ that we can improve the current known bounds on relational complexity, height and maximal size of a minimal base, denoted by $\mathrm{RC}(G)$, $\mathrm{H}(G)$ and $\mathrm{B}(G)$ respectively. In addition, we prove that a base for G of size at most $5 \log n$ can be computed in polynomial time.

In the second half of this thesis we investigate the generating graphs of permutation groups. For a 2-generated group G, the *generating graph* $\Gamma(G)$ has vertex set given by the non-identity elements of G where two elements are adjacent if and only if they generate G. Generating graphs were first introduced by Liebeck and Shalev in [42], this reinterpretation of a generation problem in terms of the generating graph enabled the use of graph theoretic results. This has prompted interest in studying various properties of the generating graphs, such as Hamiltonian cycles in [4]. One topic which has been widely studied are *cliques*, which are complete induced subgraphs of $\Gamma(G)$. Indeed, generating graphs were first used in [42] to show that for all $c < 1$, if G is a sufficiently large simple group, then $\Gamma(G)$ contains a clique of size at least c times the minimum index of a proper subgroup of G. Here we investigate the relatively less well-studied *cocliques*, which are empty induced subgraphs in $\Gamma(G)$.

Let G be a group with maximal subgroup M. Subgroups generated by elements of M must be contained in M, and so the non-identity elements of M form a coclique in $\Gamma(G)$. However it is not clear if the non-identity elements of M will form a maximal coclique. We shall see examples of both possibilities. For ease we say that M is or is not a maximal coclique rather than referring to the non-identity elements.

Let G be $\mathrm{A}_n := \mathrm{Alt}(\{1, \dots, n\})$ or $\mathrm{S}_n := \mathrm{Sym}(\{1, \dots, n\})$, and let M be either a maximal intransitive or a maximal imprimitive subgroup of G. We determine when M is a maximal coclique in $\Gamma(G)$. Showing that M is a maximal coclique is equivalent to showing that for each $x \in G \backslash M$ there exists $y \in M$ such that such that $H := \langle x, y \rangle$ is equal to G. We make considerable use of *Jordan elements*, which are elements $g \in \mathrm{S}_n$ with the property that all primitive subgroups of S_n which contain g also contain A_n. For each $x \in G \backslash M$ we construct an element $y \in M$ of suitable parity such that H is primitive and contains a Jordan element. Although the majority of the volume of this work is taken up by proving primitivity, the most challenging aspect is the construction of y.

Numerical invariants bridge the two halves of the thesis. In the first half we bound numerical invariants of primitive permutation groups. In the second we construct primitive permutation groups and use Jordan elements, some of are derived from numerical invariants, to show that these groups must be the whole of A_n or S_n. For example, for G a transitive subgroup of S_n, the *minimal degree* $\mu(G)$ is the smallest number of points in the support any non-identity element of G. In [40], Liebeck and Saxl prove that if G is a primitive group which does not contain A_n, then $\mu(G) > 2(\sqrt{n} - 1)$. Hence, in particular, if $g \in \mathrm{S}_n$ is a non-identity element and $|\mathrm{Supp}(g)| \leq 2(\sqrt{n} - 1)$, then x is a Jordan element.

In Chapter 2 we introduce the definitions, notation and preliminary lemmas used in Chapter 3. We begin by briefly covering some abstract group theory. We then define the numerical invariants that will be the focus of the first half of the thesis and prove some preliminary lemmas about these invariants. Next we give an informal summary of computational complexity. The rest of this chapter is devoted to the groups used in

Chapter 3. We cover two families of the O'Nan Scott Theorem: the almost simple and product action groups. Finally we consider some actions of these groups.

In Chapter 3 we first let $\mathbb{F} = \mathrm{GF}(q)$, let $G = \mathrm{PGL}_d(q)$, let M be the set of all $d \times d$ matrices over $\mathbb{F}$, and let Ω be the set of all m-dimensional subspaces of a $\mathbb{F}^d$. We begin by considering the action of M on Ω, and use this find an upper bound on $\mathrm{I}(G, \Omega)$ as a function of m and d. By bounding $|\Omega|$ we use the previous result to find an upper bound on $\mathrm{I}(G, \Omega)$ as a function of $|\Omega|$. We construct an irredundant and a minimal base for G, from which we obtain lower bounds on $\mathrm{I}(G, \Omega)$ and $\mathrm{B}(G, \Omega)$ as functions of m and d. Next we prove that if G is an almost simple primitive subgroup of S_n which is not large base, then $\mathrm{I}(G) < 5 \log n - 1$. Using this result we bound $\mathrm{I}(G)$ for G a product action group. By combining this work with existing results of Gill, Lodá and Spiga [28], we show that if $G \leq \mathrm{S}_n$ is a primitive group which is not large base, then $\mathrm{I}(G) < 5 \log n$. Finally we show that for each positive constant c there are infinitely many primitive groups with $\mathrm{I}(G) > c\mathrm{b}(G)$.

In the second half of the thesis we change focus from numerical invariants to generating graphs. In Chapter 4 we introduce the preliminary material for Chapters 5 and 6. We first define the intransitive and imprimitive maximal subgroups of S_n and A_n and prove some results for these maximal groups. We then prove combinatorial lemmas on block systems and cycle structures. Next we give some examples of Jordan elements and prove that subgroups of S_n which satisfy certain conditions must contain a Jordan element. Then we prove some technical results on the existence of primes with particular properties. In the penultimate section we introduce generating graphs and give some examples of maximal cocliques. Finally prove results on subgroups of S_n and 1-dimensional affine groups.

In Chapter 5 we let $\frac{n}{2} < k < n$, $G = \mathrm{S}_n$ or A_n and

$$M = \Big(\mathrm{Sym}(\{1, \ldots, k\}) \times \mathrm{Sym}(\{k+1, \ldots, n\})\Big) \cap G = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G.$$

Then M is an intransitive maximal subgroup of G. For $n \leq 11$ we determine when M is a maximal coclique in $\Gamma(G)$ computationally. For $n \geq 12$ we show that M is a maximal coclique in $\Gamma(G)$ unless $G = \mathrm{S}_n$ and $\gcd(n, k) > 1$. In addition, for $G = \mathrm{S}_n$ and $\gcd(n, k) > 1$ we show that the maximal coclique containing M is $M \cup (1, k+1)^M$.

In addition, we prove a conjecture of Cameron, Lucchini, and Roney-Dougal [14] when $G = \mathrm{A}_n$ or S_n, and n is a prime such that $n \neq \frac{q^d-1}{q-1}$ for all prime powers q and all $d \geq 2$. Namely, we show that two elements of G have identical sets of neighbours in $\Gamma(G)$ if and only if they belong to exactly the same maximal subgroups.

In Chapter 6 we continue our study of maximal cocliques in generating graphs. We let $n = mk$, let $G = \mathrm{S}_n$ or A_n and let $M = (\mathrm{S}_k \operatorname{wr} \mathrm{S}_m) \cap G$ be an imprimitive maximal subgroup of G. Here we show if $k \geq 28$ or $m \geq 27$, then M is a maximal coclique in the generating graph of G. For $x \in G \backslash M$, finding an element $y \in M$ such that $\langle x, y \rangle$ is primitive and contains a Jordan element seems to be significantly harder than in the intransitive case. The cycle types of elements in M are more restricted than those in an intransitive group. In particular elements of M are guaranteed to preserve at least one block system and often preserve many more, and elements with large support are less often Jordan elements. Because of this we introduce more cases, more number theory, more types of Jordan elements. We also use a different method of proving primitivity.

Combining the above with the work in Chapter 5 we prove the following result. Let $n = 2p$ where p is a prime greater than 29 such that $p \neq 2^a + 1$ for all $a \in \mathbb{N}$, let $G = \mathrm{S}_n$ or A_n and M is a maximal subgroup in G. Then either M is a maximal coclique in $\Gamma(G)$ or $(G, M) = (\mathrm{S}_n, \mathrm{S}_k \times \mathrm{S}_{n-k})$ for k even.

In Chapter 8, the appendix, we include some technical proofs on elements of primitive subgroups of S_n for small n, and some small cases for Chapter 5.

Chapter 2

Group actions and numerical invariants

Here we introduce the background material and preliminary results needed in Chapter 3. The first two sections define groups which we will study further. In the third and fourth sections we classify some of the possible actions of these groups. Finally in the fifth and sixth we define some numerical invariants and prove various preliminary lemmas on these invariants.

2.1 Abstract group theory

We begin with some abstract group theory which we will use to define various groups in later sections. Throughout, let n be a natural number and let $\mathrm{S}_n = \mathrm{Sym}(\{1, \ldots, n\})$.

2.1.1 Semidirect and wreath products

First we describe semidirect products which we then use to define wreath products.

Let H and K be two finite groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. For $h \in H$ and $k \in K$, let h^k denote the image of h under $\phi(k)$. Then for each $k \in K$ the map $\phi(k) : h \mapsto h^k$ for $h \in H$ is an automorphism of H. Let G be the set

$$\big\{(h, k) \bigm| h \in H, k \in K\big\},$$

and for $(h_1, k_1), (h_2, k_2) \in G$, let multiplication of G be defined by

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2^{k_1^{-1}}, k_1 k_2).$$

With this multiplication, we call G the *semidirect product* of H and K which we denote by $G = H \rtimes_\phi K$. When the action of ϕ is clear we just write $G = H \rtimes K$.

It is easily verified that $1_G = (1_H, 1_K)$ and $(h, k)^{-1} = \big((h^k)^{-1}, k^{-1}\big)$. If $\phi(k) = 1$ for all $k \in K$, then $H \rtimes_\phi K$ is the direct product $H \times K$.

Example 2.1.1. Let $H = \mathrm{S}_4$, let $K = \mathrm{S}_3 \leq H$ and let $\phi : K \mapsto \mathrm{Aut}(H)$ where $\phi(k) : h \mapsto k^{-1}hk$ for $k \in K$ and $h \in H$. Let $G = H \rtimes K$ and let

$$g_1 = \big((1,2)(3,4), (1,2,3)\big),\ g_2 = \big((1,3,4), (2,3)\big) \in G.$$

Then

$$\begin{aligned} g_1 g_2 &= \Big((1,2)(3,4) \cdot (1,3,4)^{(1,2,3)^{-1}},\ (1,2,3)(2,3)\Big) \\ &= \Big((1,2)(3,4)(1,2,3)(1,3,4)(1,3,2),\ (1,2,3)(2,3)\Big) \\ &= \Big((1,4,2),\ (1,3)\Big). \end{aligned} \qquad \triangle$$

Using the semidirect product we can define the holomorph of a group.

Definition 2.1.2. Let H be a finite group and let $\mathrm{Aut}(H)$ be the automorphism group of H. The *holomorph* of H is

$$\mathrm{Hol}(H) = H \rtimes \mathrm{Aut}(H).$$

Example 2.1.3. Let C_4 be the cyclic group of order 4 defined by

$$C_4 = \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \leq \mathrm{S}_4.$$

Then $C_4 = \langle (1,2,3,4) \rangle = \langle (1,4,3,2) \rangle$. Since automorphisms of a group map generators to generators it follows that $\mathrm{Aut}(C_4) = \{1, \sigma\}$ where 1 fixes all elements of C_4 and σ fixes id and $(1,3)(2,4)$ and interchanges $(1,2,3,4)$ and $(1,4,3,2)$. Then σ has order 2, and so $\mathrm{Aut}(C_4) = C_2$. Hence

$$\mathrm{Hol}(G) = C_4 \rtimes C_2. \quad \triangle$$

We now define the wreath product construction and a possible action, which will be used in Section 2.5. We introduce a further action in Chapter 4.

Let H and K be finite groups acting on finite sets Δ and $\Gamma = \{1, \ldots, n\}$ respectively. For $\delta \in \Delta$ and $\gamma \in \Gamma$, let δ^h and γ^k denote the images of δ and γ under $h \in H$ and $k \in K$ respectively. Then we can construct a homomorphism $\phi : K \to \mathrm{Aut}(H^n)$ where

$$\phi(k) : (h_1, h_2, \ldots, h_n) \mapsto (h_{1^{k^{-1}}}, h_{2^{k^{-1}}}, \ldots, h_{n^{k^{-1}}}).$$

Then the semidirect product $G = H^n \rtimes_\phi K$ is the *wreath product* of H by K, which we denote by $H \wr K$ or $H \operatorname{wr} K$.

Then $G = H \operatorname{wr} K$ acts on $\Omega = \Delta^n$ via the *product action* defined as follows. Let $\omega = (\delta_1, \dots, \delta_n) \in \Omega$ and let $g = \big((h_1, h_2, \dots, h_n), k\big) \in G$. Then the image of ω under g is

$$\Big(\delta_{1^{k^{-1}}}^{h_{1^{k^{-1}}}}, \dots, \delta_{n^{k^{-1}}}^{h_{n^{k^{-1}}}}\Big).$$

Example 2.1.4. Let $\Gamma = \{1,2,3,4\}$, let $\Delta = \{1,2,3\}$, and let $\Omega = \{1,2,3\}^4$. Let $K = \mathrm{Sym}(\Gamma) \cong \mathrm{S}_4$, let $H = \mathrm{Sym}(\Delta) \cong \mathrm{S}_3$ and let $G = H \operatorname{wr} K \cong \mathrm{S}_3 \operatorname{wr} \mathrm{S}_4$ act on Ω via the product action. For example let $\omega = (\omega_1, \omega_2, \omega_3, \omega_4) = (3,1,2,3) \in \Omega$ and let

$$g = \Bigg(\Big((1,2),(1,2,3),(2,3),(3,2,1)\Big),(1,4)(2,3)\Bigg) \in G.$$

Then the image of ω under g is

$$(3^{(3,2,1)}, 2^{(2,3)}, 1^{(1,2,3)}, 3^{(1,2)}) = (2,3,2,3). \quad \triangle$$

2.1.2 Insoluble subgroups of Chevalley groups

In this subsection we define soluble and insoluble groups, give a brief description of some of the Chevalley groups, and finally show that certain subgroups of these Chevalley groups are insoluble.

Let G be a finite group. A *subnormal series* for G is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = 1.$$

If G has a subnormal series as above, such that G_{i-1}/G_i is abelian for $1 \leq i \leq k$, then we call G *soluble*. If there exists no such series, then we call G *insoluble*.

Let G and H be finite groups. Then H is *involved* in G if there exist groups N and K such that $N \trianglelefteq K \leq G$ and $K/N \cong H$.

Example 2.1.5. Let $G = \langle (1,2,3,4,5,6), (2,6)(3,5) \rangle \leq \mathrm{S}_6$. Then $G \cong \mathrm{Dih}(12)$ and

$$G \rhd \langle (1,2,3,4,5,6) \rangle \rhd 1.$$

Now $G/\langle (1,2,3,4,5,6) \rangle$ and $\langle (1,2,3,4,5,6) \rangle/1$ are isomorphic to C_2 and C_6 respectively, and so both are abelian. Hence G is soluble and C_2 is involved in G. $\triangle$

We now cover two results on soluble and insoluble groups. One which we use the show that certain groups are insoluble, and one which we use later in Section 2.3.

Theorem 2.1.6 (Burnside's Theorem). *Let G be a finite group. If $|G| = p^a q^b$, where p and q are primes and a and b non-negative integers, then G is soluble.*

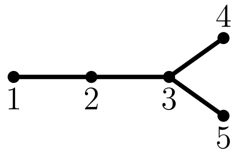
Lemma 2.1.7. *Let H be a non-abelian simple group. If H is involved in a group G, then G is insoluble.*

Proof. If G is soluble, then all subgroups and quotients of G are soluble, see for example [24, Theorem 10.2(a)]. Hence if G has a subgroup or quotient that is insoluble, then it follows that G is insoluble.

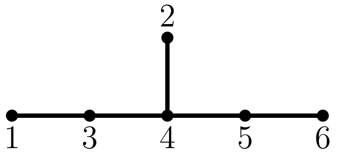
Since H is simple, it follows that the only subnormal series is $H \triangleright 1$. Now $H/1 = H$ is non-abelian, and so H is insoluble. Since H is involved in G there exist groups N and K satisfying $N \trianglelefteq K \leq G$ and $K/N \cong H$. Hence K is insoluble since it contains H as a quotient group, and in turn G is insoluble since it contains K as a subgroup. □

We now take a brief foray into Dynkin diagrams and Chevalley groups. Here we only cover the information which is needed in Chapter 3, in particular we show that certain parabolic subgroups of particular Chevalley groups are insoluble. For a more comprehensive exposition see [20].

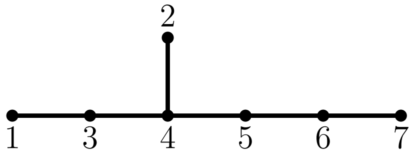
The following graphs (omitting the labelling of vertices) are the D_5, E_6 and E_7 Dynkin diagrams. These correspond to the Chevalley groups $D_5(q) \cong \mathrm{P}\Omega^+_{10}(q)$, $E_6(q)$ and $E_7(q)$, where q is a prime power and these groups are defined over the field $\mathbb{F} = \mathrm{GF}(q)$.



D_5



E_6



E_7

The labelling of the vertices (here we use the notational convention of [2]) is used to label subgroups as follows.

Let $\mathcal{G}$ be the Dynkin diagram D_5, E_6 or E_7, and let G be the corresponding Chevalley group $D_5(q)$, $E_6(q)$ or $E_7(q)$. Let v_i be the vertex of $\mathcal{G}$ labelled by i, and let $\mathcal{G}_i$ be the subgraph of $\mathcal{G}$ given by removing v_i and all edges incident with v_i. Then $\mathcal{G}_i$ corresponds to a subgroup P_i, called a parabolic subgroup of G. Each connected component of $\mathcal{G}_i$ will be another Dynkin diagram (for a complete list of Dynkin diagrams see [20]). If $\mathcal{G}_i$ is connected, then P_i involves the Chevalley group corresponding to $\mathcal{G}_i$.

For example, if $\mathcal{G} = E_6$, then $\mathcal{G}_1$ and $\mathcal{G}_6$ are both D_5. Hence the parabolic subgroups P_1 and P_6 of $E_6(q)$ both involve $D_5(q)$.

Lemma 2.1.8. *Let G be a Chevalley group and let H be a parabolic subgroup of G. If*

$$(G, H) \in \big\{(E_6(q), P_1), (E_6(q), P_6), (E_7(q), P_7)\big\},$$

then H is insoluble.

Proof. If $\mathcal{G} = E_6$, then $\mathcal{G}_1 = \mathcal{G}_6 = D_5$, and so $P_1, P_6 \leq E_6(q)$ involve $D_5(q)$. If $\mathcal{G} = E_7$, then $\mathcal{G}_7 = E_6$ and so $P_7 \leq E_7(q)$ involves $E_6(q)$.

Both $D_5(q)$ and $E_6(q)$ are non-abelian simple groups, and so in all cases H is insoluble by Lemma 2.1.7. □

2.1.3 Primitive and large-base groups

Here we briefly define blocks, primitive groups and large-base groups. For more detail and examples of blocks see Section 4.2.

Definition 2.1.9. Let Ω be a finite set and let G be a transitive subgroup of $\mathrm{Sym}(\Omega)$. A set $\Delta \subseteq \Omega$ is a *block* for G if for all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. If $|\Delta| = 1$ or $\Delta = \Omega$, then Δ is a *trivial* block, otherwise Δ is *non-trivial.*

If G has no non-trivial blocks, then G is *primitive*, otherwise G is *imprimitive.*

Example 2.1.10. Let $\Omega = \{1, 2, \dots, 8\}$, let $\Delta = \{1, 5\}$, let $g = (1, 2, 3, 4, 5, 6, 7, 8)$ and $h = (2, 8)(3, 7)(4, 6)$ be elements of $\mathrm{Sym}(\Omega)$, and let $G = \langle g, h\rangle$. It is clear that G is transitive. If $f \in G$, then

$$\Delta^f \in \{\Delta, \Delta^g, \Delta^{g^2}, \Delta^{g^3}\} = \big\{\{1, 5\}, \{2, 6\}, \{3, 7\}, \{4, 8\}\big\}.$$

Hence Δ is a block for G and so G is imprimitive.

Now let $n \geq 5$, let $\Omega = \{1, \dots, n\}$, and let $G = \mathrm{A}_n = \mathrm{Alt}(\Omega)$. Suppose that $\Delta \subseteq \{1, 2, \dots, n\}$ is a non-trivial block, and so there exist distinct points $\alpha, \beta \in \Delta$ and $\gamma \notin \Delta$. Since G is 2-transitive, it follows that there exists $g \in G$ such that $\alpha^g = \alpha$ and $\beta^g = \gamma$. Hence $\alpha \in \Delta \cap \Delta^g$ and $\gamma \in \Delta^g \backslash \Delta$, a contradiction. Hence G has no non-trivial blocks, and so is primitive. △

The following definition was prompted by a result of Liebeck which we cover later in Section 2.2.

Definition 2.1.11. Let G be a primitive subgroup of degree n. Then G is *large base* if G is a subgroup of $\mathrm{S}_t \operatorname{wr} \mathrm{S}_r$ containing $(\mathrm{A}_t)^r$, where the action of S_t is on k-element subsets of $\{1, \dots, t\}$ and the wreath product has the product action of degree $n = \binom{t}{k}^r$.

2.2 Numerical invariants

In this section we introduce various numerical invariants which we bound for certain groups in Chapter 3. We also cover some examples, motivational and contextual history of numerical invariants.

Throughout this section let Ω be a finite set and let $G \leq \mathrm{Sym}(\Omega)$. For a sequence $\Lambda = (\lambda_1, \dots, \lambda_k) \in \Omega^k$, let G_Λ be the pointwise stabiliser of Λ in G. For a set $\Delta \subseteq \Omega$, let G_Δ and $G_{(\Delta)}$ be the setwise and pointwise stabiliser of Δ in G. For $H \leq G$, let $[G : H]$ be the index of H in G. Let log be to the base 2.

Definition 2.2.1. A *base* for G is a sequence $\Lambda = (\lambda_1, \dots, \lambda_k) \in \Omega^k$ such that, $G_\Lambda = 1$. The *minimal base size*, denoted $\mathrm{b}(G, \Omega)$ or just $\mathrm{b}(G)$ if the meaning is clear, is the minimum length of a base for G. A base for G is *minimal* if no proper subsequence is a base, that is $G_\Gamma \neq 1$ for all subsequences Γ of Λ. The maximal size of a minimal base for G is denoted by $\mathrm{B}(G, \Omega)$ or $\mathrm{B}(G)$.

Example 2.2.2. Let $n \geq 5$ and let $\Omega = \{1, 2, \dots, n\}$.

First let $G = \mathrm{S}_n$, let $k \leq n-2$ and let $\Lambda \in \Omega^k$. Then there exist distinct points $\alpha, \beta \in \Omega$ which are not terms of Λ. Hence $(\alpha, \beta) \in G_\Lambda$, and so $\mathrm{b}(G) > n-2$. Since the only element of G fixing $n-1$ points of Ω is the identity, it follows that $\mathrm{b}(G) = n-1$.

Now let $G = \mathrm{A}_n$, let $k \leq n-3$ and let $\Lambda \in \Omega^k$. Then there exist distinct points $\alpha, \beta, \gamma \in \Omega$ which are not in Λ, and so $(\alpha, \beta, \gamma) \in G_\Lambda$. Let $\Lambda \in \Omega^{n-2}$ be a sequence of distinct points. Then there are exactly two distinct points $\alpha, \beta \in \Omega$ which are not in Λ. Then $(S_n)_\Lambda = \langle (a, b) \rangle$, and so $G_\Lambda = 1$. Hence $\mathrm{b}(G) = n-2$.

Finally let $n = 2m > 4$ and let

$$G = \big\langle (2, n)(3, 2m-1) \cdots (m, m+2), (1, 2, \dots, 2m) \big\rangle.$$

Then $G \cong \mathrm{Dih}(2n)$. The only non-identity element of G_1 is the reflection through the vertices 1 and $m+1$. Hence

$$G_1 = \big\langle (2, n)(3, n-1) \cdots (m, m+2) \big\rangle = G_{(1,m+1)},$$

and so neither (1) nor $(1, m+1)$ is a base. However $G_{(1,2)} = 1 = G_{(1,m+1,2)}$, and so $(1, 2)$ is a minimal base, and $(1, m+1, 2)$ is a base but not a minimal base. $\triangle$

We now discuss some motivation for the study of bases. Let $g, h \in G$ and let $\Lambda = (\lambda_1, \dots, \lambda_k) \in \Omega^k$ be a base for G. If $\lambda_i^g = \lambda_i^h$ for $1 \leq i \leq k$, then $gh^{-1} \in G_\Lambda = 1$, and so $g = h$. Hence each element of G can be defined and stored by its action on $|\Lambda|$, rather than $|\Omega|$, points. If $|\Lambda|$ is significantly smaller than $|\Omega|$, as for $\mathrm{Dih}(2n)$ but not for

S_n or A_n, then this results in a computational saving. As a result base size has important applications in computational group theory, see for example [51] for the importance of a base and strong generating set.

In [38] Liebeck proves the following landmark result.

Theorem 2.2.3. *Let G be a primitive subgroup of S_n. Then one of the following holds.*

(i) *G is large base,*

(ii) $\mathrm{b}(G) < 9 \log n$.

Very recently in [47] Moscatiello and Roney-Dougal improved Liebeck's bound by showing that if G is a primitive subgroup of S_n which is not large base, then either $G = \mathrm{M}_{24}$ in its 5-transitive action of degree 24, or $\mathrm{b}(G) \leq \lceil \log n \rceil + 1$.

We now cover a definition and result which link the two halves of this thesis. For G a subgroup of S_n, the *minimal degree* $\mu(G)$ is the smallest number of points in the support any non-identity element of G.

For example $\mu(\mathrm{S}_n) = 2$, $\mu(\mathrm{A}_n) = 3$ and $\mu(\langle (1, 2, \ldots, p) \rangle) = p$.

Theorem 2.2.4 ([40, Theorem 2])**.** *Let G be a primitive subgroup of S_n which is not large base. Then $\mu(G) \geq \frac{1}{3}n$.*

In the same paper as the previous theorem, Liebeck and Shalev also prove the following corollary. If G is a primitive subgroup of S_n and $\mu(G) \leq 2(\sqrt{n} - 1)$, then G contains A_n. We rephrase this result in Theorem 4.3.4(iii) for use in Chapters 5 and 6 where we study generation in S_n and A_n.

Theorems 2.2.3 and 2.2.4 are of the same form; for a primitive subgroup of S_n which is not large base, they bound a numerical invariant as a function of n. One area of interest is to prove similar results for other numerical invariants. This is the focus of Chapter 3, where we study the following numerical invariants.

Definition 2.2.5. Let Ω be a set of size n, let G be a subgroup of $\mathrm{Sym}(\Omega)$ and let $\Gamma \subseteq \Omega$. Then Γ is *independent* if $G_{(\Sigma)} \neq G_{(\Gamma)}$ for each $\Sigma \subsetneq \Gamma$. The *height* of G, denoted $H(G, \Omega)$ or $\mathrm{H}(G)$, is the maximum size of an independent set.

Definition 2.2.6. Let $\Lambda = (\lambda_1, \ldots, \lambda_k) \in \Omega^k$ be a base for G. Then Λ is *irredundant* if

$$G > G_{\lambda_1} > G_{\lambda_1,\lambda_2} > \cdots > G_{\lambda_1,\lambda_2,\ldots,\lambda_k} = 1.$$

If no other irredundant base is longer than Λ, then Λ is a *maximal irredundant base* and we denote its length by $\mathrm{I}(G, \Omega)$ or $\mathrm{I}(G)$.

Observe that if Λ is an irredundant base, all points of Λ are distinct. Hence the following notation is well defined.

Notation 2.2.7. For Λ an irredundant base containing λ, let $\Lambda\backslash\{\lambda\}$ be the subsequence of Λ given by omitting λ.

The maximum length of a chain of subgroups of G is denoted by $\ell(G)$. It is easily seen that $\mathrm{I}(G) \leq \ell(G)$.

Theorem 2.2.8 ([16, Theorem 1])**.** $\ell(\mathrm{S}_n) \leq \frac{3n}{2}$.

The following shows how various numerical invariants are related.

Lemma 2.2.9 ([28, Equation 1.1])**.** *Let G be a transitive subgroup of* S_n*. Then*

$$\mathrm{b}(G) \leq \mathrm{B}(G) \leq \mathrm{H}(G) \leq \mathrm{I}(G) \leq \mathrm{b}(G)\log n.$$

Proof. Clearly $\mathrm{b}(G) \leq \mathrm{B}(G)$. Let $k = \mathrm{B}(G)$ with corresponding base $\Lambda = (\lambda_1, \dots, \lambda_k)$. Let $\Delta = \{\lambda_1, \dots, \lambda_k\}$. Since Λ is a minimal base it follows that Λ contains no repetitions and so Δ has size k, and that no subsequence of Λ is a base and so $G_{(\Gamma)} \neq G_{(\Delta)}$ for all $\Gamma \subsetneq \Delta$. Therefore Δ is an independent set of size k, and so $\mathrm{B}(G) = k \leq \mathrm{H}(G)$.

Now let $\Delta = \{\lambda_1, \dots, \lambda_l\}$ be an independent set of maximal size. Then $l = \mathrm{H}(G)$ and we have the following chain of subgroups

$$G \geq G_{\lambda_1} \geq G_{\lambda_1,\lambda_2} \geq \cdots \geq G_{\lambda_1,\dots,\lambda_l}.$$

Since G is transitive, it follows that $G > G_{\lambda_1}$. If there exists $2 \leq i \leq l$ such that $G_{\lambda_1,\dots,\lambda_{i-1}} = G_{\lambda_1,\dots,\lambda_{i-1},\lambda_i}$, then $G_{(\Delta)} = G_{(\Delta\backslash\{\lambda_i\})}$, a contradiction since Δ is an independent set for G. Hence

$$G > G_{\lambda_1} > \cdots > G_{\lambda_1,\dots,\lambda_l}.$$

For $i \geq 1$ if $G_{\lambda_1,\dots,\lambda_{l+i-1}} \neq 1$, then let λ_{l+i} be a point in the largest orbit of $G_{\lambda_1,\dots,\lambda_{l+i-1}}$. Hence there exists $t \geq 0$ such that

$$G > G_{\lambda_1} > G_{\lambda_1,\lambda_2} > \cdots > G_{\lambda_1,\dots,\lambda_{l+t}} = 1.$$

Thus $(\lambda_1, \dots, \lambda_{l+t})$ is an irredundant base for G, and so $\mathrm{H}(G) = l \leq l + t \leq \mathrm{I}(G)$.

Finally let $m = \mathrm{I}(G)$ and $b = \mathrm{b}(G)$, and let $\Lambda = (\lambda_1, \dots, \lambda_m)$ and $(\delta_1, \dots, \delta_b)$ be corresponding bases. Then

$$G > G_{\lambda_1} > G_{\lambda_1,\lambda_2} > \cdots > G_{\lambda_1,\dots,\lambda_m} = 1 \text{ and}$$

$$G > G_{\delta_1} > G_{\delta_1,\delta_2} > \cdots > G_{\delta_1,\dots,\delta_b} = 1.$$

Hence $[G : G_{\lambda_1}] \geq 2$ and $[G_{\lambda_1,\ldots,\lambda_{i-1}} : G_{\lambda_1,\ldots,\lambda_i}] \geq 2$ for $2 \leq i \leq m$. Therefore

$$|G| = [G : G_{\lambda_1}][G_{\lambda_1} : G_{\lambda_1,\lambda_2}] \cdots [G_{\lambda_1,\ldots,\lambda_{m-1}} : G_{\lambda_1,\ldots,\lambda_m}] \geq 2^m = 2^{\mathrm{I}(G)}.$$

Since $G \leq \mathrm{S}_n$, it follows that $[G : G_{\delta_1}] \leq n$ and $[G_{\delta_1,\ldots,\delta_i} : G_{\delta_1,\ldots,\delta_{i+1}}] \leq n$ for $1 \leq i \leq b-1$. Hence

$$|G| = [G : G_{\delta_1}][G_{\delta_1} : G_{\delta_1,\delta_2}] \cdots [G_{\delta_1,\ldots,\delta_{b-1}} : G_{\delta_1,\ldots,\delta_b}] \leq n^b = n^{\mathrm{b}(G)}.$$

Therefore $2^{\mathrm{I}(G)} \leq |G| \leq n^{\mathrm{b}(G)}$, and so the result then follows by taking logarithms base 2 on both sides. □

We now define one final numerical invariant, relational complexity. Informally, this is a measure of when local properties of an object imply global properties. This has been studied extensively in model theory, see for example [37]. A rephrasing of the definition, to make it easier to work with permutation groups, was introduced more recently in [19].

Definition 2.2.10. Let $k, l \in \mathbb{N}$ with $k \leq l$ and let $\Gamma = (\gamma_1, \ldots, \gamma_l), \Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l$. Then Γ and Λ are *k-subtuple complete* or *k-equivalent* with respect to $G \leq \mathrm{Sym}(\Omega)$, denoted $\Gamma \sim_k \Lambda$, if for every subset of k indices $\{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, l\}$ there exists $g \in G$ such that

$$(\gamma_{i_1}^g, \ldots, \gamma_{i_k}^g) = (\lambda_{i_1}, \ldots, \lambda_{i_k}).$$

The *relational complexity* of G, denoted $\mathrm{RC}(G)$, is the smallest k such that for all $l \geq k$ and all $\Gamma, \Lambda \in \Omega^l$, if $\Gamma \sim_k \Lambda$ then $\Lambda \in \Gamma^G$.

Here $\Gamma \sim_k \Lambda$ is the local property, and $\Lambda \in \Gamma^G$ is the global property.

Example 2.2.11. Let $\Omega = \{1, 2, 3, 4, 5, 6\}$, let $G = \mathrm{S}_6$ or A_6, and let $\Gamma = (\gamma_1, \ldots, \gamma_5) = (1, 2, 3, 4, 5), \Lambda = (\lambda_1, \ldots, \lambda_5) = (1, 2, 3, 4, 6) \in \Omega^5$.

Since both S_6 and A_6 are 3-transitive, it follows that $\Gamma \sim_3 \Lambda$. For example let $i_1 = 1$, $i_2 = 2$ and $i_3 = 5$. Then the corresponding subsequences are $\Gamma' = (\gamma_1, \gamma_2, \gamma_5) = (1, 2, 5)$ and $\Lambda' = (\lambda_1, \lambda_2, \lambda_5) = (1, 2, 6)$, and the elements $(5, 6) \in \mathrm{S}_6$ and $(4, 5, 6) \in \mathrm{A}_6$ map Γ' to Λ'.

We claim that if $G = \mathrm{S}_6$, then $\Lambda \in \Gamma^G$, and if $G = \mathrm{A}_6$, then $\Lambda \notin \Gamma^G$. If $\Gamma^g = \Lambda$ then, g fixes $1, 2, 3$ and 4, and maps 5 to 6. Hence $g = (5, 6)$ is the only element of S_6 satisfying $\Gamma^g = \Lambda$. Since $g \in \mathrm{S}_6 \backslash \mathrm{A}_6$ the claim follows.

Hence if $G = \mathrm{A}_6$, then $\mathrm{RC}(G) > 3$ since $\Gamma \sim_3 \Lambda$ and $\Lambda \notin \Gamma^G$. △

The following gives the range of possible values of relational complexity.

Lemma 2.2.12. *Let $n \geq 3$ and let G be a non-trivial subgroup of* S_n. *Then*

$$2 \leq \mathrm{RC}(G) \leq n-1.$$

Proof. Let $\Omega = \{1, 2, \ldots, n\}$ and let $k = \mathrm{RC}(G)$. Then for all $l \in \mathbb{N}$ and all $\Gamma = (\gamma_1, \ldots, \gamma_l), \Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l$, if $\Gamma \sim_k \Lambda$ then $\Lambda \in \Gamma^G$.

Since G is non-trivial there exist distinct points $\alpha, \beta \in \Omega$ and $g \in G$ such that $\alpha^g = \beta$. Hence $(\alpha, \alpha) \sim_1 (\alpha, \beta)$. However $(\alpha, \beta) \notin (\alpha, \alpha)^G$, and so $\mathrm{RC}(G) \neq 1$ and the lower bound holds. In addition, it follows that if $k \geq 2$ and $\Gamma \sim_k \Lambda$, then $\gamma_i = \gamma_j$ if and only if $\lambda_i = \lambda_j$. Hence $\gamma_i^g = \lambda_i$ if and only if $\gamma_j^g = \lambda_j$, and so we may assume without loss of generality that Γ and Λ are repetition free. Therefore Γ and Λ have length at most n.

Let $\Gamma = (\gamma_1, \ldots, \gamma_n), \Lambda = (\lambda_1, \ldots, \lambda_n) \in \Omega^n$ be repetition free. If $\Gamma \sim_{n-1} \Lambda$, then in particular there exists $g \in G$ with $(\gamma_1^g, \ldots, \gamma_{n-1}^g) = (\lambda_1, \ldots, \lambda_{n-1})$. Since $G \leq \mathrm{S}_n$, it follows that $\gamma_n^g = \lambda_n$ and so $\Gamma^g = \Lambda$. Hence if $\Gamma \sim_{n-1} \Lambda$, then $\Lambda \in \Gamma^G$, and so $\mathrm{RC}(G) \leq n-1$. □

Now we consider examples of groups which show that the bounds in the above lemma are tight. Note that as part of the proof above we showed that if $\Gamma = (\gamma_1, \ldots, \gamma_l)$, $\Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l$ and $\Gamma \sim_2 \Lambda$, then $\gamma_i = \gamma_j$ implies that $\lambda_i = \lambda_j$.

Example 2.2.13. Let p be a prime, let $\Omega = \{1, \ldots, p\}$, and let $G = \langle (1, \ldots, p) \rangle \leq \mathrm{S}_p$. Hence $G \cong C_p$. Let $\Gamma = (\gamma_1, \ldots, \gamma_l), \Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l$ with $\Gamma \sim_2 \Lambda$. From $\Gamma \sim_2 \Lambda$ it follows that for $2 \leq k \leq l$ there exists $g_k \in G$ such that $\gamma_1^{g_k} = \lambda_1$ and $\gamma_k^{g_k} = \lambda_k$. Since there is a unique element $g \in G$ with $\gamma_1^g = \lambda_1$, it follows that $g = g_k$ for $2 \leq k \leq l$. Hence $\Gamma^g = \Lambda$ and so $\mathrm{RC}(G) = 2$. △

Example 2.2.14. Let $n \geq 5$ and let $\Omega = \{1, \ldots, n\}$.

First let $G = \mathrm{S}_n$, and let $\Gamma, \Lambda \in \Omega^l$ with $\Gamma \sim_2 \Lambda$. Since G is n-transitive it follows that there exists $g \in G$ satisfying $\Gamma^g = \Lambda$. Hence $\Lambda \in \Gamma^G$ and so $\mathrm{RC}(G) = 2$.

Now let $G = \mathrm{A}_n$. Let $\Gamma = (1, 2, \ldots, n-2, n-1, n), \Lambda = (1, 2, \ldots, n-2, n, n-1) \in \Omega^n$. Since G is $(n-2)$-transitive it follows that $\Lambda \sim_{n-2} \Gamma$. The only element of S_n mapping Γ to Λ is $(n-1, n)$. Since $(n-1, n) \notin G$ it follows that $\Lambda \notin \Gamma^G$ and so $\mathrm{RC}(G) > n-2$. Now $\mathrm{RC}(G) \leq n-1$ by Lemma 2.2.12, and $\mathrm{RC}(G) = n-1$. △

Hence both S_n and C_p have relational complexity 2. In [18] Cherlin gives examples of primitive groups with relational complexity 2, called *binary groups*, and conjectures that this list is complete. In a dramatic breakthrough Gill, Liebeck and Spiga proved this conjecture [26].

We now compare relational complexity to some of the other numerical invariants. Let $n \geq 5$. Then $\mathrm{b}(\mathrm{S}_n) = \mathrm{b}(\mathrm{A}_n) + 1$ by Example 2.2.2, whereas $\mathrm{RC}(\mathrm{S}_n) = 2$ and $\mathrm{RC}(\mathrm{A}_n) = n - 1$ by Example 2.2.14.

Let $H \leq G \leq \mathrm{S}_n$ and let Λ be a minimal base for G. Then $G_\Lambda = 1$, and so $H_\Lambda = 1$. Hence Λ is a base (although not necessarily minimal) for H, and so $\mathrm{b}(H) \leq \mathrm{b}(G)$. There is no such general rule that relates $\mathrm{RC}(H)$ to $\mathrm{RC}(G)$. With the action of S_n on k-subsets being an exception - see [27], the current results on height and relational complexity would seem to imply that $\mathrm{RC}(G)$ is either equal or close to $\mathrm{H}(G) + 1$. This observation prompts the following lemma.

Lemma 2.2.15 ([28, Lemma 2.1])**.** *Let G be a primitive subgroup of* S_n*. Then*

$$\mathrm{RC}(G) \leq \mathrm{H}(G) + 1.$$

2.3 Lemmas on irredundant bases

We now collect results about bases and the relation between maximal irredundant bases and other group statistics.

Throughout this section let Ω be a finite set. For $G \leq \mathrm{Sym}(\Omega)$ and a fixed sequence $(\omega_1, \ldots, \omega_l) \in \Omega^l$, let $G^{(0)} = G$ and $G^{(i)} = G_{\omega_1,\ldots,\omega_i}$ for $1 \leq i \leq l$.

Lemma 2.3.1. *Let G be a subgroup of* S_n*.*

(i) *If G is insoluble, then* $\mathrm{I}(G) < \log|G| - 1$*.*

(ii) *If G is transitive and $n \geq 5$, then* $\mathrm{I}(G) < \log|G| - 1$*.*

(iii) *If G is transitive and $b = \mathrm{b}(G)$, then* $\mathrm{I}(G) \leq (b-1)\log n + 1$*.*

Proof. If $\Lambda = (\lambda_1, \ldots, \lambda_t)$ is either a minimal base, or a maximal irredundant base, for G, then

$$|G| = [G^{(0)} : G^{(1)}] \cdots [G^{(t-1)} : G^{(t)}] \quad \text{and} \quad 2 \leq [G^{(i)} : G^{(i+1)}] \leq n \text{ for } 0 \leq i \leq t. \tag{2.1}$$

In addition, if G is transitive then by the Orbit-Stabilizer Theorem

$$[G^{(0)} : G^{(1)}] = n. \tag{2.2}$$

(i) Let $l = \mathrm{I}(G)$, let $p_1, p_2, \ldots, p_r$ be distinct increasing primes and let $a_1, a_2, \ldots, a_r$ be positive integers such that $|G| = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Then $a = a_1 + a_2 + \cdots + a_r$ is the number of prime divisors of $|G|$ including multiplicity. By setting Λ to be a maximal irredundant base in (2.1), it follows that $a \geq l$.

Since G is insoluble, Theorem 2.1.6 implies that $r \geq 3$ and so $p_r \geq 5 > 2^2$. Hence $p_i^{a_i} \geq 2^{a_i}$ for $1 \leq i \leq r-1$, and $p_r^{a_r} > 2^{a_r+1}$. Therefore

$$|G| > 2^{a_1} \cdot 2^{a_2} \cdot \cdots \cdot 2^{a_r+1} = 2^{a+1},$$

and so $\log |G| > a+1 \geq l+1$. Thus $\mathrm{I}(G) = l < \log |G| - 1$.

(ii) Let $l = \mathrm{I}(G)$. Then by setting Λ to be a maximal irredundant base in (2.1) and (2.2), it follows that

$$|G| = n \cdot [G^{(1)} : G^{(2)}] \cdots [G^{(1)} : G^{(2)}] \geq n \cdot 2^{l-1}. \tag{2.3}$$

Hence if $n \geq 5$ then $|G| \geq 5 \cdot 2^{l-1} > 2^{l+1}$. Therefore $\log |G| > l+1$, and so $\mathrm{I}(G) = l < \log |G| - 1$.

(iii) Let $b = \mathrm{b}(G)$. Then by setting Λ to be a minimal base in (2.1) and 2.2 it follows that

$$|G| = n \cdot [G^{(1)} : G^{(2)}] \cdots [G^{(1)} : G^{(2)}] \leq n \cdot n^{b-1} = n^b.$$

Combining the above with (2.3) gives $n \cdot 2^{l-1} \leq |G| \leq n^b$. Hence $2^{l-1} \leq n^{b-1}$, and so $\mathrm{I}(G) = l \leq (b-1)\log n + 1$.

□

Lemma 2.3.2. *Let G be a subgroup of* $\mathrm{Sym}(\Omega)$*, let $l \geq 1$ and let $\Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l$. Then there exists a subsequence Σ of Λ such that Σ can be extended to an irredundant base and $G_\Sigma = G_\Lambda$.*

Proof. The sequence Λ cannot be extended to an irredundant base if and only if there exists a subsequence $\lambda_i, \ldots, \lambda_{i+j}$ of Λ such that $j \geq 1$ and

$$G^{(i)} = G^{(i+1)} = \cdots = G^{(i+j)}.$$

Let Σ be the subsequence of Λ given by deleting all such $\lambda_{i+1}, \ldots, \lambda_{i+j}$. Since $G^{(i)} = G^{(i+j)}$ it follows that $G_\Lambda = G_\Sigma$. □

Lemma 2.3.3. *Let $H \leq G \leq \mathrm{Sym}(\Omega)$ and let $\Delta \subseteq \Omega$ be a H-orbit. Then $\mathrm{I}(H, \Delta) \leq \mathrm{I}(G, \Omega)$.*

Proof. Let $k = \mathrm{I}(H, \Delta)$ with corresponding base $\Lambda = (\lambda_1, \ldots, \lambda_k) \in \Delta^k$. Then

$$G > G_{\lambda_1} > \cdots > G_{\lambda_1, \ldots, \lambda_k}.$$

Let $K = G_{\lambda_1, \ldots, \lambda_k}$. If $K = \mathrm{id}$ then Λ is an irredundant base for G and so $\mathrm{I}(G, \Omega) \geq \mathrm{I}(H, \Delta)$. If $K \neq \mathrm{id}$ then $\mathrm{I}(K, \Omega) = l \geq 1$ with corresponding base $(\mu_1, \ldots, \mu_l)$. In which case

$(\lambda_1, \ldots, \lambda_k, \mu_1, \ldots, \mu_l)$ is an irredundant base for G and so

$$\mathrm{I}(G, \Omega) \geq k + l > k = \mathrm{I}(H, \Delta). \quad \square$$

The following two lemmas recently appeared in [28], for the second we include our own independent proof.

Lemma 2.3.4. *[28, Lemma 2.6] Let H_1 and H_2 be non-identity permutation groups on Ω_1 and Ω_2, then*

$$\mathrm{I}(H_1 \times H_2, \Omega_1 \times \Omega_2) = \mathrm{I}(H_1, \Omega_1) + \mathrm{I}(H_2, \Omega_2) - 1.$$

Lemma 2.3.5. *[28, Lemma 2.8] Let $N \trianglelefteq G \leq \mathrm{S}_n$. Then*

$$\mathrm{I}(G) \leq \mathrm{I}(N) + \ell(G/N).$$

Proof. Let $\mathrm{I}(G) = l$ with a corresponding base $\Lambda = (\omega_1, \ldots, \omega_l)$. Then

$$G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(l)} = 1,$$

and so

$$GN = G^{(0)}N \geq G^{(1)}N \geq G^{(2)}N \geq \cdots \geq G^{(l)}N = N.$$

Let $I = \{1 \leq i \leq l \mid G^{(i-1)}N = G^{(i)}N\}$ and $J = \{1 \leq j \leq l \mid G^{(j-1)}N > G^{(j)}N\}$.

If $i \in I$, then by the Second Isomorphism Theorem

$$G^{(i-1)}/(G^{(i-1)} \cap N) \cong G^{(i-1)}N/N = G^{(i)}N/N \cong G^{(i)}/(G^{(i)} \cap N).$$

Since $G^{(i)} \cap N = N^{(i)}$ this implies that $\frac{|G^{(i-1)}|}{|N^{(i-1)}|} = \frac{|G^{(i)}|}{|N^{(i)}|}$, and so $\frac{|G^{(i-1)}|}{|G^{(i)}|} = \frac{|N^{(i-1)}|}{|N^{(i)}|}$. Therefore $G^{(i-1)} > G^{(i)}$ if and only if $N^{(i-1)} > N^{(i)}$. Hence by letting $I = \{i_1, \ldots, i_k\}$, it follows that

$$N > N^{(i_1)} > N^{(i_2)} > \cdots > N^{(i_k)} = 1$$

and so $\mathrm{I}(N, \Omega) \geq k$.

If $j \in J$, then $G^{(j-1)}N > G^{(j)}N$, and so $G^{(j-1)}N/N > G^{(j)}N/N$. Since $I \dot{\cup} J = \{1, 2, \ldots, l\}$, we can let $J = \{j_1, \ldots, j_{l-k}\}$. Recall that $G^{(j_i)} = G_{\omega_1, \omega_2, \ldots, \omega_{j_i}}$. Hence

$$GN/N > G^{(j_1)}N/N > G^{(j_2)}N/N > \cdots > G^{(j_{l-k})}N/N,$$

and so $\ell(G/N) \geq l - k$. $\square$

Corollary 2.3.6. *Let $N \trianglelefteq G \leq \mathrm{S}_n$ such that $[G:N] = p$ for some prime p. Then*

$$\mathrm{I}(N) \leq \mathrm{I}(G) \leq \mathrm{I}(N) + 1.$$

Proof. The lower bound holds by Lemma 2.3.3. If $N \trianglelefteq G$ and $[G : N] = p$, then $G/N \cong C_p$. Since the only proper subgroup of C_p is 1 it follows that $\ell(C_p) = 1$. Hence the upper bound follows from Lemma 2.3.5. □

2.4 Computational Complexity

Let G be a primitive subgroup of S_n which is not large base. In Chapter 3 we bound some of the numerical invariants discussed in the previous section as a function on n. As a corollary, we prove a result on the computational complexity of calculating a base of a certain size for G.

We now give a very brief and informal summary of computational complexity theory. A *decision problem* is a problem for which the answer is yes or no. An *instance* of the problem is one specific case of the problem. We give some of the hierarchy of difficulty for decision problems. To determine the hierarchy of a problem we use Turing machines, which are mathematical models of computers. It is universally believed that for any algorithm there exists a Turing machine that carries out the algorithm. Here we are particularly interested in *deterministic* Turing machines, where for any input at most one action is performed. A *non-deterministic* Turing machine is one where an input can result in multiple actions being carried out in parallel. Unless otherwise stated, assume that we are using a deterministic Turing machine.

We use the following “big O notation” to categorise functions.

Definition 2.4.1. Let $f, g : \mathbb{R} \to \mathbb{R}$. If there exists $c, n_0 \in \mathbb{R}$ such that $|f(n)| \leq cg(n)$ for all $n \geq n_0$, then we say $f(n) = O(g(n))$.

We now define the hierarchy. Suppose that we have a decision problem where an instance input has size n. If there exists $k \in \mathbb{N}$, independent of n, such that any instance can be solved by a Turing machine in $O(n^k)$ steps, then this problem is in P. If there exists $l \in \mathbb{N}$ such that a possible solution can be checked to be correct in $O(n^l)$ steps, then the problem is in NP. Problems in NP can be solved in polynomial time by a non-deterministic Turing machine. Since constructing a solution automatically checks its correctness, it follows that NP contains P. It is not currently known if P=NP, although it is widely believed that NP is a wider class of problems than P. Problems are said to be NP-hard if they are at least as hard as those in NP. Finally, a problem is NP-complete if it lies in both NP and NP-hard.

Example 2.4.2. Let $t \in \mathbb{N}$ and $X \subset \mathbb{N}$. Determining if there exists $x \in X$ such that $x > t$ is a problem in P. Indeed for each $x \in X$ we need only test whether or not $x > t$. Hence this problem can be solved in a number of steps which is polynomial in the input size. An instance of this problem would be $t = 7$ and $X = \{1, 9, 6\}$.

Suppose instead that we wish to determine if there exists $\{x_1, \dots, x_s\} \subseteq X$ such that $x_1 + \dots + x_s = t$. This is a problem in NP which is thought not to be in P. A naive approach would be to consider all sums of subsets of X. There are 2^n subsets of X, and so this approach would require at least $O(2^n)$ steps. This gives some indication as to why this problem is computationally harder than the last. However, given a potential solution $\{x_1, \dots, x_r\} \subseteq X$, it takes polynomially many steps to calculate $x_1 + \cdots + x_s$ and then compare this to t. Hence checking a candidate solution takes polynomial time. $\triangle$

A *greedy algorithm* is an algorithm where at each stage we make a locally optimal choice. Let Ω be a finite set and let $G = G^{(0)} \leq \mathrm{Sym}(\Omega)$. The following is a greedy algorithm for constructing a base for G.

Step 1 Let λ_1 be a point from a largest orbit of $G^{(0)}$, and let $G^{(1)} = G^{(0)}_{\lambda}$.

Step $i \geq 2$ We have a sequence of points $(\lambda_1, \dots, \lambda_{i-1})$ and $G^{(i-1)} = G_{\lambda_1, \dots, \lambda_{i-1}}$.
If $G^{(i-1)}$ has orbits of size at least 2, then let λ_i be a point in a largest orbit of $G^{(i-1)}$.
If all orbits of $G^{(i-1)}$ have size 1, then stop.

Suppose that the algorithm terminates at step t. Then $G > G^{(1)}$, and $G^{(i)} > G^{(i+1)}$ for $1 \leq i \leq t-1$, and $G^{(t)} = 1$. Hence $(\lambda_1, \dots, \lambda_t)$ an irredundant base, and so $\mathrm{b}(G) \leq t \leq \mathrm{I}(G)$. Observe that $|G^{(i+1)}| = \frac{|G^{(i)}|}{r_i}$ for $0 \leq i \leq t-1$, where r_i is the size of the orbit of $G^{(i)}$ containing λ_{i+1}. Therefore at each stage λ_{i+1} is chosen to ensure that $G^{(i+1)}$ is as small as possible.

Let G be a primitive group which is not large base. In [1] Blaha proved that computing a minimal base for a permutation group is NP-hard. Deciding if there exists a base of size at most t is NP-complete. Blaha also showed that using the greedy algorithm above, we can compute a base of size $O(\mathrm{b}(G) \log\log n)$ in polynomial time. Hence using Theorem 2.2.3 it follows that if G is a primitive subgroup of S_n which is not large base, then we can construct a base of size $O(\log n \log\log n)$ in polynomial time. We improve this bound in Chapter 3.

2.5 Linear algebra and linear groups

In this section we define various classical groups which will be used in the next section. For more detail see [3], [36] and [55]. We begin by introducing some matrix notation and matrix groups.

Throughout this section let p be a prime, let $f \in \mathbb{N}$ and let $q = p^f$. Let $\mathbb{F}$ be the field $\mathrm{GF}(q)$, and let $\mathbb{F}^*$ be the non-zero elements of $\mathbb{F}$. Then the characteristic of $\mathbb{F}$, $\mathrm{char}(\mathbb{F})$, is p.

Let V be a d-dimensional vector space over $\mathbb{F}$. Let $e_1, \ldots, e_d$ be the standard basis for V, so that e_i has 1 in the i^{th} position and 0 elsewhere. For U a vector space over $\mathbb{F}$ let $\dim(U)$ be the dimension of U over $\mathbb{F}$.

Let $\mathbb{M}_{m,d}(\mathbb{F})$ be the set of all $m \times d$ matrices over $\mathbb{F}$. For $A \in \mathbb{M}_{m,d}(\mathbb{F})$ we write $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq d}}$ to mean that we denote the entry of A in the i^{th} row and j^{th} column by a_{ij}. When the dimensions of A are clear we write $A = (a_{ij})$. It is easily verified that $\mathbb{M}_{m,d}(\mathbb{F})$ is a vector space over $\mathbb{F}$, and $\dim(\mathbb{M}_{m,d}(\mathbb{F})) = md$.

We shall identify V with the set of d-dimensional row vectors over $\mathbb{F}$, let $M = \mathbb{M}_{d,d}(\mathbb{F})$, and let I be the $d \times d$ identity matrix. Then M acts on V by right multiplication. For example, let $v = (v_1, \ldots, v_d) \in V$ and let $A = (a_{ij}) \in M$. Then

$$vA = \left(\sum_{i=1}^{d} a_{i1} v_i, \sum_{i=1}^{d} a_{i2} v_i, \ldots, \sum_{i=1}^{d} a_{id} v_i \right) \in V.$$

2.5.1 Linear and semilinear groups

We call groups introduced in this section and the next *classical groups*. We begin with linear and semilinear groups.

A map $g : V \to V$ is a *linear transformation* from V to V if for all $u, v \in V$ and all $c \in \mathbb{F}$

$$(u+v)g = ug + vg \qquad \text{and} \qquad (cv)g = c(vg).$$

The *general linear group*, denoted by $\mathrm{GL}(V)$, is the set of all invertible linear transformations from V to V. If we fix a basis of V, then we may realise $\mathrm{GL}(V)$ as $\mathrm{GL}_d(q)$, the group of $d \times d$ invertible matrices with entries in $\mathbb{F}$. Then $\mathrm{GL}_d(q)$ acts on V by right multiplication. We can then define $\mathrm{SL}_d(q)$, the *special linear group* on V, to be the group of matrices in $\mathrm{GL}_d(q)$ with determinant 1.

An element $g \in \mathrm{GL}_d(q)$ is a *scalar transformation* if there exists $c \in \mathbb{F}^*$ such that $vg = cv$ for all $v \in V$. Let Z be the set of all scalar transformations of V. Then it can easily be shown that Z is the centre of $\mathrm{GL}_d(q)$, which we denote $\mathrm{Z}(\mathrm{GL}_d(q))$, and that $Z = \mathbb{F}^* I$. The *projective linear group* on V is

$$\mathrm{PGL}_d(q) = \mathrm{GL}_d(q)/Z.$$

The *projective special linear group* on V is

$$\mathrm{PSL}_d(q) = \mathrm{SL}_d(q)Z/Z.$$

We now move from linear maps to semilinear maps. A map $g : V \to V$ is a *semilinear transformation* if there exists $\alpha \in \mathrm{Aut}(\mathbb{F})$, such that for all $u, v \in V$ and all $c \in \mathbb{F}$

$$(u+v)g = ug + vg \quad \text{and} \quad (cv)g = c^{\alpha}(vg).$$

We call α the *associated automorphism* of g. If α is the identity, then g is a linear transformation. Then *general semilinear group* $\Gamma\mathrm{L}_d(q)$ is the group of all invertible semilinear transformations of V. The *projective semilinear group* is

$$\mathrm{P}\Gamma\mathrm{L}_d(q) = \Gamma\mathrm{L}_d(q)/Z.$$

Let $\Phi : x \mapsto x^p$ be the Frobenius automorphism of $\mathbb{F}$. Then Φ has order f and $\mathrm{Aut}(\mathbb{F}) = \langle \Phi \rangle$. Hence if we let C_f be the cyclic group of order f, then $\mathrm{Aut}(\mathbb{F}) \cong C_f$ and

$$\mathrm{P}\Gamma\mathrm{L}_d(q) = \mathrm{PGL}_d(q) \rtimes C_f. \tag{2.4}$$

For $A \in \mathrm{GL}_d(q)$ denote the inverse transpose of A by A^{-T}. Then the map $\iota : \mathrm{GL}_d(q) \to \mathrm{GL}_d(q)$, where $\iota : A \mapsto A^{-T}$ for $A \in \mathrm{GL}_d(q)$, is an automorphism of $\mathrm{GL}_d(q)$ called the *inverse-transpose automorphism.* It is easily seen that $\iota(Z) = Z$ and $\iota(\mathrm{SL}_d(q)) = \mathrm{SL}_d(q)$. Let $g \in \mathrm{PSL}_d(q)$, then $g = AZ$ for some $A \in \mathrm{GL}_d(q)$. Hence $\iota(g) = \iota(AZ) = A^{-T}Z \in \mathrm{PSL}_d(q)$, and so $\iota \in \mathrm{Aut}(\mathrm{PSL}_d(q))$. In addition, Φ and ι commute. By [36, (2.1.14)]

$$\mathrm{Aut}(\mathrm{PSL}_d(q)) = \begin{cases} \mathrm{P}\Gamma\mathrm{L}_2(q) & \text{if } d = 2, \\ \mathrm{P}\Gamma\mathrm{L}_d(q) \rtimes \langle \iota \rangle & \text{if } d \geq 3. \end{cases} \tag{2.5}$$

Let $m \leq d$ and let η be a map from the set of m-dimensional spaces to the set of $(d-m)$-dimensional spaces which acts as follows on U an m-dimensional space

$$\eta(U) = \{v \in V \mid uv^T = 0 \text{ for all } u \in U\}. \tag{2.6}$$

2.5.2 Classical forms

In this section we introduce classical forms, which will be used to define more classical groups.

Let α be an automorphism of $\mathbb{F}$. Then a map $B : V \times V \to \mathbb{F}$ is an α-*sesquilinear* form on V if for all $c_1, c_2 \in \mathbb{F}$ and $u_1, u_2, v_1, v_2 \in V$

$$\begin{aligned} B(c_1u_1 + c_2u_2, v_1) &= c_1B(u_1, v_1) + c_2B(u_2, v_1) \text{ and} \\ B(u_1, c_1v_1 + c_2v_2) &= c_1^\alpha B(u_1, v_1) + c_2^\alpha B(u_1, v_2). \end{aligned}$$

We now define special types of α-sesquilinear forms.

- If α is the identity, then B is a *bilinear form*.
- For all $u, v \in V$, if $B(u, v) = 0$ implies that $B(v, u) = 0$, then B is *reflexive*.
- If $B(u, v)^\alpha = B(v, u)$ for all $u, v \in V$ and α has order 2, then B is *α-Hermitian*.
- Let B be bilinear. If $B(u, v) = B(v, u)$ for all $u, v \in V$, then B is *symmetric*. If $B(u, v) = -B(v, u)$ for all $u, v \in V$, then B is *skew-symmetric*. If $B(u, u) = 0$ for all $u \in V$, then B is *alternating*.
- If $B(u, v) = 0$ for all $u \in V$ implies that $v = 0$, then B is *non-degenerate* (or equivalently if $B(u, v) = 0$ for all $v \in V$ implies that $u = 0$).

Let U be a subspace of V and let B be a non-degenerate α-sesquilinear form on V. A vector $v \in V$ is *isotropic* if $B(v, v) = 0$. If B restricted to U is the zero map, then U is *totally isotropic* (or *t.i.*). If B restricted to U is non-degenerate, then U is *non-degenerate* (or *n.d.*). If there exist linearly independent vectors $u, v \in U$ such that $U = \langle u, v \rangle$, $B(u, u) = 0 = B(v, v)$ and $B(u, v) = 1$, then we say that U is a *hyperbolic line* with *hyperbolic pair* (u, v).

Let B be an α-sesquilinear form. We use B to define elements of $\mathrm{GL}_d(q)$ and $\Gamma\mathrm{L}_d(q)$ with specific properties. We later show that for some types of B, the sets of all such elements form subgroups of $\mathrm{GL}_d(q)$ and $\Gamma\mathrm{L}_d(q)$. First let $g \in \mathrm{GL}_d(q)$. We say that g is an *isometry* of B, or that g *preserves* B, if $B(ug, vg) = B(u, v)$ for all $u, v \in V$. If there exists $c \in \mathbb{F}^*$ such that $B(ug, vg) = cB(u, v)$ for all $u, v \in V$, then g is a *similarity* of B. Now let $h \in \Gamma\mathrm{L}_d(q)$ with associated automorphism σ. If there exists $c \in \mathbb{F}^*$ such that $B(uh, vh) = cB(u, v)^\sigma$ for all $u, v \in V$, then h is a *semisimilarity* of B.

We now introduce one further type of map which we will use to define classical groups. A map $Q : V \to \mathbb{F}$ is a *quadratic form* on V, if $Q(cv) = c^2Q(v)$ for all $v \in V$ and $c \in \mathbb{F}$ and the function $B : V \times V \to \mathbb{F}$ defined by

$$B(u, v) = Q(u + v) - Q(u) - Q(v)$$

is a bilinear form. We call B the *polarisation* of Q.

If $\mathrm{char}(\mathbb{F}) \neq 2$, then from

$$B(u,u) = Q(2u) - 2Q(u) = 2^2Q(u) - 2Q(u) = 2Q(u)$$

it follows that $Q(v) = \frac{1}{2}B(v,v)$. Hence Q can be recovered from B. If $\mathrm{char}(\mathbb{F}) = 2$, then each bilinear form is the polarisation of many quadratic forms. Let Q be a quadratic form with polarisation B. If $B(u,v) = 0$ for all $v \in V$ implies that $u = 0$, then we say that Q is *non-degenerate*.

Let $v \in V$, let U be a subspace of V, let Q be a non-degenerate form on V. If $Q(v) = 0$, then v is *totally singular*. If each element of U is totally singular, then U is *totally singular* (or *t.s.*).

Let Q be a quadratic form. As for bilinear forms, we define certain subsets of $\mathrm{GL}_d(q)$ and $\Gamma\mathrm{L}_d(q)$. First let $g \in \mathrm{GL}_d(q)$. If $Q(ug) = Q(u)$ for all $u \in V$, then we say that g is an *isometry* of Q, or that g *preserves* Q. If there exists $c \in \mathbb{F}^*$ such that $Q(ug) = cQ(u)$ for all $u \in V$, then g is a *similarity* of Q. Now let $h \in \Gamma\mathrm{L}_d(q)$ with associated automorphism α. If there exists $c \in \mathbb{F}^*$ such that $Q(uh) = cQ(u)^\alpha$ for all $u \in V$, then h is a *semisimilarity* of Q.

In this paragraph only, let V be a vector space over $\mathbb{F} = \mathrm{GF}(q^2)$. Then the map $\sigma : x \mapsto x^2$ for $x \in \mathbb{F}$ is an automorphism of $\mathbb{F}$. By [36, Prop 2.3.1 and 2.3.2] the isometry groups of any pair of non-degenerate σ-hermitian forms are conjugate in $\mathrm{GL}_d(q^2)$. Hence if we fix a non-degenerate σ-hermitian form B, then the following unitary groups are unique up to conjugation. The group of all isometries of B is the *isometry group* of B, denoted $\mathrm{GU}_d(q)$. The *special isometry group* of B is $\mathrm{SU}_d(q) = \mathrm{GU}_d(q) \cap \mathrm{SL}_d(q^2)$. The group of all semisimilarities of B is the *semisimilarity group* of B, denoted $\Gamma\mathrm{U}_d(q)$. Let $Z = \mathrm{Z}(\mathrm{GL}_d(q^2))$. We then have the corresponding three projective groups $\mathrm{PGU}_d(q) = \mathrm{GU}_d(q)/(Z \cap \mathrm{GU}_d(q))$, $\mathrm{PSU}_d(q) = \mathrm{SU}_d(q)/(Z \cap \mathrm{SU}_d(q))$ and $\mathrm{P}\Gamma\mathrm{U}_d(q) = \Gamma\mathrm{U}_d(q)/Z$.

We return to V being a vector space with underlying field $\mathbb{F} = \mathrm{GF}(q)$. Here we define the sympletic groups. Let B be a non-degenerate alternating form on V. Then set of all *similarities*; of all *isometries*; and of all *semisimilarities* of B, are $\mathrm{GSp}_d(q)$, $\mathrm{Sp}_d(q)$, and $\Gamma\mathrm{Sp}_d(q)$. We then have the corresponding three projective groups $\mathrm{PGSp}_d(q) = \mathrm{GSp}_d(q)/Z$, $\mathrm{PSp}_d(q) = \mathrm{Sp}_d(q)/(Z \cap \mathrm{Sp}_d(q))$ and $\mathrm{P}\Gamma\mathrm{Sp}_d(q) = \Gamma\mathrm{Sp}_d(q)/Z$.

Let Q be a non-degenerate quadratic form of V with associated bilinear form B. We define the following subsets of V. Let δ_{ij} be the Kronecker-Delta function and recall that $\dim(V) = d$.

(i) A *hyperbolic* subset is $\{v_1, \ldots, v_r, u_1, \ldots, u_r\} \subseteq V$ with $d = 2r$ such that for $i, j \in$

$\{1, 2, \dots r\}$

$$Q(v_i) = Q(u_i) = 0 \text{ and } B(v_i, u_j) = \delta_{ij}.$$

(ii) A *parabolic* subset is $\{v_1, \dots, v_r, u_1, \dots, u_r, w\} \subseteq V$ with $d = 2r + 1$, such that both $\langle v_1, \dots, v_r \rangle$ and $\langle u_1, \dots, u_r \rangle$ are totally singular, w is non-singular and for all $i, j \in \{1, 2, \dots r\}$

$$Q(v_i) = Q(u_i) = 0, \;\; B(v_i, u_j) = \delta_{ij} \text{ and } B(v_i, w) = B(u_i, w) = 0.$$

(iii) An *elliptic* subset is $\{v_1, \dots, v_r, u_1, \dots, u_r, w, z\} \subseteq V$ with $d = 2r + 2$ such that $Q(z) = \eta$ where $x^2 + x + \eta$ is irreducible in $\mathbb{F}[x]$, both $\langle v_1, \dots, v_r \rangle$ and $\langle u_1, \dots, u_r \rangle$ are totally singular, and for all $i, j \in \{1, 2, \dots r\}$

$$Q(v_i) = Q(u_i) = 0,$$

$$B(v_i, u_j) = \delta_{ij}, \quad B(v_i, w) = B(v_i, z) = B(u_i, w) = B(u_i, z) = 0 \text{ and } B(w, z) = 1.$$

Lemma 2.5.1. *(Prop 2.5.3 [36]) Let Q be a non-degenerate quadratic form over V with associated bilinear form B. Then V has either a hyperbolic, a parabolic or an elliptic basis.*

Let

$$\epsilon = \begin{cases} + & \text{if } d \text{ is even and the basis of } V \text{ is hyperbolic,} \\ \text{blank} & \text{if } d \text{ is odd and the basis of } V \text{ is parabolic,} \\ - & \text{if } d \text{ is even and the basis of } V \text{ is elliptic.} \end{cases}$$

Let Q be a fixed non-degenerate quadratic form. Denote the *similarity group* of Q by $\mathrm{GO}^{\epsilon}_d(q)$; the *isometry group* of Q by $\mathrm{O}^{\epsilon}_d(q)$; the *special isometry group* of Q by $\mathrm{SO}^{\epsilon}_d(q)$; the *semisimilarity group* of Q by $\Gamma\mathrm{O}^{\epsilon}_d(q)$; and $\Omega^{\epsilon}_d(q)$ to be an index 2 subgroup of $\mathrm{SO}^{\epsilon}_d(q)$ (this is uniquely defined for $(d, q, \epsilon) \neq (4, 2, +)$).

For $X \in \{\mathrm{GO}^{\epsilon}_d(q), \mathrm{O}^{\epsilon}_d(q), \mathrm{SO}^{\epsilon}_d(q), \Gamma\mathrm{O}^{\epsilon}_d(q), \Omega^{\epsilon}_d(q)\}$ we define the corresponding projective groups

$$PX = X/(X \cap Z).$$

The following theorem classifies when some of the classical groups that we have defined are simple. Some restrictions on d are to omit duplications due to isomorphism - see [36, Proposition 2.9.1].

Theorem 2.5.2 ([55, See for example Theorems 4.5, 8.8, 10.20, 11.48])**.**

(i) *If $G = \mathrm{PSL}_d(q)$, then G is simple if and only if $(d, q) \neq (2, 2), (2, 3)$.*

(ii) *If* $G = \mathrm{PSp}_d(q)$*, then* G *is simple if and only if* $(d, q) \neq (2, 2), (2, 3), (4, 2)$.

(iii) *If* $G = \mathrm{PSU}_d(q)$*, then* G *is simple if and only if* $(d, q) \neq (2, 2), (2, 3), (3, 2)$.

(iv) *If* $G = \mathrm{P}\Omega^{\epsilon}_d(q)$*, then* G *is simple for all* $d \geq 7$.

2.6 Almost simple and product action groups

In this section we cover two families of the O'Nan-Scott Theorem. This result, which was independently proved by Michael O'Nan and Leonard Scott in 1979, divides the primitive groups into eight types. We begin with some preliminary material.

Definition 2.6.1. Let G be a group. Then H is a *minimal normal subgroup* of G, if $1 \neq H \trianglelefteq G$ and the only normal subgroups of G contained in H are 1 and H.

The *socle* of G, denoted $\mathrm{soc}(G)$, is the subgroup generated by all minimal normal subgroups of G.

A group G acting transitively on a set Ω acts *regularly* if $G_\omega = 1$ for each $\omega \in \Omega$.

Example 2.6.2. Let $n \in \mathbb{N}$ and let $\Omega = \{1, \dots, n\}$.

First let C_n be the cyclic group of order n generated by $(1, 2, \dots, n)$. Then C_n is clearly transitive and $(C_n)_\omega = 1$ for all $\omega \in \Omega$. Hence C_n acts regularly on Ω.

Now let $n = 2m + 1$ be odd, and let

$$G = \big\langle (1, 2, \dots, 2m + 1), (2, 2m + 1)(3, 2m) \dots (m, m + 1) \big\rangle.$$

Then $G \cong \mathrm{Dih}(2n)$, G is transitive and $G_1 = \langle (2, 2m + 1)(3, 2m) \dots (m, m + 1) \rangle$. Hence G does not act regularly on Ω. △

Let G be a finite group acting on a set Ω. Then G acts *faithfully* if the only element of G fixing Ω pointwise is the identity. Equivalently, we can identify G with a subgroup of $\mathrm{Sym}(\Omega)$.

Let Ω be a finite set of size n and let G be a primitive subgroup of $\mathrm{Sym}(\Omega)$. Then $S := \mathrm{soc}(G) \cong T^m$ for a simple group T. The following gives two of the families of the O'Nan-Scott Theorem.

Definition 2.6.3. Let G be a primitive subgroup of $\mathrm{Sym}(\Omega)$ with minimal normal but not regular socle $S \cong T^m$.

(i) G is type AS if $m = 1$, so that

$$T \trianglelefteq G \leq \mathrm{Aut}(T).$$

(ii) G is type PA if $m > 1$ and there exists a finite set Δ and a primitive AS group $U \leq \mathrm{Sym}(\Delta)$ with socle T such that

$$T^m \trianglelefteq G \leq U \,\mathrm{wr}\, \mathrm{Sym}(m)$$

and $\Omega = \Delta^m$.

For the full statement of the theorem and more in-depth analysis see [23].

The following gives an example of groups of type AS and PA. Let $\mathrm{S}_n = \mathrm{Sym}(\{1, \dots, n\})$ and $\mathrm{A}_n = \mathrm{Alt}(\{1, \dots, n\})$.

Example 2.6.4. Let $n \geq 7$ and let $T = \mathrm{A}_n$. Then T is simple and $\mathrm{Aut}(T) = \mathrm{S}_n$. Therefore $T \trianglelefteq \mathrm{S}_n \leq \mathrm{Aut}(T)$, and so S_n is an example of a group of type AS.

Now let $T = \mathrm{PSL}_d(q)$ for $(d, q) \neq (2, 2), (2, 3)$, and so by Theorem 2.5.2 T is simple. By (2.5)

$$T \triangleleft \mathrm{PGL}_d(q) \leq \mathrm{Aut}(\mathrm{PSL}_d(q)),$$

and so $\mathrm{PGL}_d(q)$ is also of type AS.

Let $G = \mathrm{S}_5 \,\mathrm{wr}\, \mathrm{S}_4$ act with product action on $\Omega = \{1, 2, 3, 4, 5\}^4$. Then G is an example of a group of type PA. △

Recall that G is of type *AS* if $T \trianglelefteq G \leq \mathrm{Aut}(T)$ where T is simple and not regular. Since T is not regular, it follows by Example 2.6.2 that T is not cyclic and so is a non-abelian simple group. Now $\mathrm{S}_1, \dots, \mathrm{S}_4$ are soluble, and so by Lemma 2.1.7 involve no non-abelian simple groups. Hence we have the following result.

Lemma 2.6.5. *Let $G \leq \mathrm{Sym}(\Omega)$. If G is of type AS, then $|\Omega| \geq 5$.*

The next lemma follows immediately from the definition of large-base groups

Lemma 2.6.6. *Let G and U be as in Definition 2.6.3(ii). If U is large base then so is G.*

2.7 Classical groups and subspace actions

Let G be an almost simple classical group with socle G_0. Hence G_0 is as in Theorem 2.5.2. In this section we classify certain actions of G for use in Chapter 3.

Throughout, let $q = p^f$ be a prime power, let $m, d \in \mathbb{N}$ with $1 \leq m \leq \frac{d}{2}$, and let V be a d-dimensional vector space over $\mathbb{F} = \mathrm{GF}(q)$.

Definition 2.7.1. Let $\mathcal{PG}_m(V)$ be the set of all m-dimensional subspaces of V.

An elementary counting argument can be used to prove the following.

Lemma 2.7.2. *Let $1 \leq m \leq \frac{d}{2}$ and let $n(d,m,q) = |\mathcal{PG}_m(\mathbb{F}^d)| = |\mathcal{PG}_m(V)|$. Then*

$$n(d,m,q) = \frac{\prod_{i=d-m+1}^{d}(q^i-1)}{\prod_{i=1}^{m}(q^i-1)}.$$

Let $G \leq \mathrm{PGL}_d(q)$. Then G acts on $\mathcal{PG}_m(V)$ via $U^x = \{u^x \mid u \in U\}$ for $U \in \mathcal{PG}_m(V)$ and $x \in G$. We now prove some lemmas about the action of groups on $\mathcal{PG}_m(V)$, we begin with a definition.

Definition 2.7.3. Let G be a group acting on two sets Ω and Γ. These actions are *equivalent* if there exists a bijection $\lambda : \Omega \to \Gamma$ such that

$$\lambda(\alpha^x) = (\lambda(\alpha))^x \quad \text{for all } \alpha \in \Omega \text{ and } x \in G.$$

Lemma 2.7.4. *Let $G \leq \mathrm{P\Gamma L}_d(q)$. Then the action of G on $\mathcal{PG}_m(V)$ is equivalent to the action of G on $\mathcal{PG}_{d-m}(V)$.*

Proof. Let $U \in \mathcal{PG}_m(V)$, let $x \in \mathrm{P\Gamma L}_d(q)$, and let $\eta : \mathcal{PG}_m(V) \to \mathcal{PG}_{d-m}(V)$ be the map described in (2.6). Then

$$\begin{aligned}(\eta(U))^x &= \{v^x \in V \mid uv^T = 0 \text{ for all } u \in U\}\\ &= \{v \in V \mid u(v^{x^{-1}})^T = 0 \text{ for all } u \in U\}\\ &= \{v \in V \mid u^x v^T = 0 \text{ for all } u \in U\}\\ &= \eta(U^x).\end{aligned}$$

□

Lemma 2.7.5. *Let G be an almost simple group with socle $\mathrm{PSL}_d(q)$ such that $G \not\leq \mathrm{P\Gamma L}_d(q)$. If $m = 1$ or if $m < \frac{d}{2}$, then G does not act on $\mathcal{PG}_m(V)$.*

Proof. If $d = 2$ then $\mathrm{Aut}(\mathrm{PSL}_d(q)) = \mathrm{P\Gamma L}_d(q)$ by (2.5), and so all almost simple groups with socle $\mathrm{PSL}_d(q)$ are contained in $\mathrm{P\Gamma L}_d(q)$. Hence assume that $m < \frac{d}{2}$, and so $d \geq 3$. Therefore $G \leq \mathrm{P\Gamma L}_d(q) \rtimes \langle \iota \rangle$ by (2.5). Since $G \not\leq \mathrm{P\Gamma L}_d(q)$ it follows that there exists $h \in \mathrm{P\Gamma L}_d(q)$ such that $h\iota \in G$. Suppose for a contradiction that G acts on $\mathcal{PG}_m(V)$, let $U \in \mathcal{PG}_m(V)$ and let H be the stabilizer of U in G. Then for all $g \in G$ we have that H^g is the stabilizer of $U^g \in \mathcal{PG}_m(V)$. However $H^{h\iota}$ is the stabilizer of $U^{h\iota} \in \mathcal{PG}_{d-m}(V)$, a contradiction. □

The following definition will be used to define another set on which classical groups can act.

Definition 2.7.6. Let U and W be subspaces of the vector space V. Then V is the *direct sum* of U and W, if $U \cap W = \underline{0}$ and $V = \{u + w \mid u \in U \text{ and } w \in W\}$. We write

$V = U \oplus W$.

Definition 2.7.7. We introduce two subsets of $\mathcal{PG}_m(V) \times \mathcal{PG}_{d-m}(V)$:

$$\Omega_m^{\oplus} = \Big\{ \{U, W\} \;\Big|\; U, W \leq V,\ \dim U = m,\ \dim W = d-m \text{ with } m < \frac{d}{2} \text{ and } U \oplus W = V \Big\}, \text{ and}$$
$$\Omega_m^{<} = \Big\{ \{U, W\} \;\Big|\; U, W \leq V,\ \dim U = m,\ \dim W = d-m \text{ with } m < \frac{d}{2} \text{ and } U \leq W \Big\}.$$

Lemma 2.7.8 ([7, Table 4.1.2])**.** *Let $\Omega_m^{\oplus}$ and $\Omega_m^{<}$ be as defined above. Then*

$$|\Omega_m^{\oplus}| = \frac{q^{m(d-m)} \prod_{i=d-m+1}^{d}(q^i - 1)}{\prod_{i=1}^{m}(q^i - 1)} \quad \textit{and} \quad |\Omega_m^{<}| = \frac{\prod_{i=d-2m+1}^{d}(q^i - 1)}{\prod_{i=1}^{m}(q^i - 1)^2}.$$

Lemma 2.7.9. *Let $\Omega = \Omega_m^{\oplus}$ or $\Omega_m^{<}$. Then $|\Omega| > 2|\mathcal{PG}_m(V)|$.*

Proof. Combining Lemmas 2.7.2 and 2.7.8 gives

$$|\Omega_m^{\oplus}| = q^{m(d-m)}|\mathcal{PG}_m(V)| \quad \text{and} \quad |\Omega_m^{<}| = \frac{\prod_{i=d-2m+1}^{d-m}(q^i - 1)}{\prod_{i=1}^{m}(q^i - 1)}|\mathcal{PG}_m(V)|.$$

Since $\frac{d}{2} > m$, it follows that $d > 2m$ and so $d - 2m + i \geq i + 1$ for $1 \leq i \leq m$. Hence the result follows since

$$q^{m(d-m)} \geq q^{m(m+1)} > 2$$

and

$$\begin{aligned} \frac{\prod_{i=d-2m+1}^{d-m}(q^i - 1)}{\prod_{i=1}^{m}(q^i - 1)} &= \frac{(q^{d-m} - 1)}{(q - 1)} \cdot \prod_{i=1}^{m-1} \frac{(q^{d-2m+i} - 1)}{(q^{i+1} - 1)} \\ &\geq \frac{(q^{d-m} - 1)}{(q - 1)} \\ &= q^{d-m-1} + \cdots + q + 1 \\ &> 2. \end{aligned}$$

□

For a classical group, the *natural module* is the module which the group is defined over. For example, if $G = \mathrm{GL}_d(q)$, then $V = \mathbb{F}^d$ is its natural module. Primitive actions of almost simple groups can be divided into two types, standard and non-standard, which are as follows.

Definition 2.7.10. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive almost simple group with socle G_0 and point stabilizer H. The action of G on Ω is *standard* if, up to equivalence of actions, one of the following holds, and is *non-standard* otherwise.

(i) $G_0 = \mathrm{Alt}(l)$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, l\}$.

(ii) G_0 and Ω are as in Table 2.1.

(iii) $G_0 = \mathrm{PSp}_d(2^f)$ and $H \cap G_0 = \mathrm{O}^{\pm}_d(2^f)$.

In the following table we introduce certain actions which we will use later in Lemma 2.7.14.

Case	$\boldsymbol{G_0}$	$\boldsymbol{\Omega}$	**Conditions**
1	$\mathrm{PSL}_d(q)$	all m-subspaces	$m \leq \frac{d}{2}$
2	$\mathrm{PSL}_d(q)$	$\Omega_m^{\oplus}$	$d \geq 3$
3	$\mathrm{PSL}_d(q)$	$\Omega_m^{<}$	$d \geq 3$
4	$\mathrm{PSU}_d(q)$	t.i. m-subspaces	$m \leq \frac{d}{2}$
5	$\mathrm{PSU}_d(q)$	n.d. m-subspaces	$m < \frac{d}{2}$
6	$\mathrm{PSp}_d(q)$	t.i. m-subspaces	$m \leq \frac{d}{2}$
7	$\mathrm{PSp}_d(q)$	n.d. m-subspaces	$m < \frac{d}{2}$, m even
8	$\mathrm{P\Omega}_d^+(q)$	t.s. m-subspaces	$m \leq \frac{d}{2}$
9	$\mathrm{P\Omega}_d^-(q)$	t.s. m-subspaces	$m < \frac{d}{2}$
10	$\mathrm{P\Omega}_d(q)$	t.s. m-subspaces	d, q odd, $m < \frac{d}{2}$
11	$\mathrm{P\Omega}_d^\epsilon(q)$	n.s. 1-subspaces	d, q even
12	$\mathrm{P\Omega}_d^+(q)$	n.d. hyperbolic m-subspaces	$m < \frac{d}{2}$, m even
13	$\mathrm{P\Omega}_d^+(q)$	n.d. elliptic m-subspaces	$m < \frac{d}{2}$, m even
14	$\mathrm{P\Omega}_d^+(q)$	n.d. parabolic m-subspaces	$m < \frac{d}{2}$, mq odd
15	$\mathrm{P\Omega}_d^-(q)$	n.d. elliptic m-subspaces	m even
16	$\mathrm{P\Omega}_d^-(q)$	n.d. parabolic m-subspaces	$m < \frac{d}{2}$, mq odd
17	$\mathrm{P\Omega}_d(q)$	n.d. hyperbolic m-subspaces	m even, dq odd
18	$\mathrm{P\Omega}_d(q)$	n.d. elliptic m-subspaces	m even, dq odd

Table 2.1: Classical groups acting on subspaces

We now cover some lemmas which we will use to categorise the primitive almost simple groups. In [13, Theorem 2] Burness et al. proved a significant result on base size for certain families of groups. Combining this result with Definition 2.7.10 and [43, Table 3.4.1] gives the following theorem.

Theorem 2.7.11. *Let G be an almost simple group with socle G_0 acting primitively on a finite set Ω. Then one of the following holds.*

(i) $\mathrm{b}(G, \Omega) \leq 6$ *or* $G = \mathrm{M}_{24}$ *in its natural action on* $\{1, \ldots, 24\}$.

(ii) *G is standard.*

Lemma 2.7.12. *Let $d \geq 2$, let $G_0 = \mathrm{PSU}_d(q)$, $\mathrm{PSp}_d(q)$ or $\mathrm{P\Omega}_d^\epsilon(q)$, and let G be a primitive almost simple group with socle G_0 acting on a G-orbit of totally isotropic, totally* *singular, or non-degenerate m-spaces. Then either $G_0 = \mathrm{P}\Omega_8^+(q)$, or $G \leq \mathrm{P\Gamma L}_d(q)$.*

Proof. By [36, Theorem 2.1.4] either $G \leq \mathrm{P\Gamma L}_d(q)$, $G_0 = \mathrm{P}\Omega_8^+(q)$ or $G_0 = \mathrm{PSp}_4(q)$ with q even. By [3, Table 8.14], if $G_0 = \mathrm{PSp}_4(q)$ and $\Omega \subseteq \mathcal{PG}_m(V)$, then G does not induce a graph isomorphism, and so $G \leq \mathrm{P\Gamma L}_d(q)$. □

The following lemma is given in [28] and proved in [43, Appendix A].

Lemma 2.7.13 ([28, Lemma 7.14])**.** *Let G be a primitive almost simple classical group with socle $G_0 = \mathrm{PSU}_d(q)$, $\mathrm{PSp}_d(q)$ or $\mathrm{P}\Omega_d^\epsilon(q)$. If G acts on an orbit Ω of m-spaces as in Table 2.1, then either $G_0 = \mathrm{P}\Omega_d^+(q)$ and $m = \frac{d}{2}$; or $|\Omega| > q^{\frac{1}{2}m(d-m)}$.*

We now give a categorisation of primitive almost simple groups which we use in Chapter 3.

Lemma 2.7.14. *Let G be a primitive almost simple group acting on a set Ω with socle G_0. Then up to equivalence of actions one of the following holds:*

(I) $\mathrm{b}(G,\Omega) \leq 6$ *or $G = \mathrm{M}_{24}$ in its natural action on* $\{1,\dots,24\}$*;*

(II) $G_0 = \mathrm{Alt}(l)$ *and Ω is an orbit of subsets or partitions of* $\{1,\dots,l\}$*;*

(III) $G_0 = \mathrm{PSL}_d(q)$ *and* $\Omega = \mathcal{PG}_m(V)$ *with* $m \leq \frac{d}{2}$*;*

(IV) $G_0 = \mathrm{PSL}_d(q)$ *and* $\Omega = \Omega_m^\oplus$*;*

(V) $G_0 = \mathrm{PSL}_d(q)$ *and* $\Omega = \Omega_m^<$*;*

(VI) $G_0 = \mathrm{PSp}_d(2^f)$ *and Ω is the set of cosets of* $\mathrm{N}_G(\mathrm{O}_d^\pm(2^f))$ *in G;*

(VII) $G_0 = \mathrm{P}\Omega_8^+(q)$*;*

(VIII) $G_0 = \mathrm{P}\Omega_d^+(q)$ *with* $d \geq 10$ *and* $\Omega \subseteq \mathcal{PG}_{\frac{d}{2}}(V)$*; or*

(IX) $G \leq \mathrm{P\Gamma L}_d(q)$ *and* $\Omega \subseteq \mathcal{PG}_m(V)$ *such that* $d \geq 3$, $m \leq \frac{d}{2}$ *and* $|\Omega| > q^{\frac{1}{2}m(d-m)}$.

Proof. By Theorem 2.7.11 either G is as in Case (I) , (II) or (VI), or G_0 and Ω are as in Table 2.1.

If G is as in Case 1, 2 or 3 of Table 2.1, then G is as in Case (III), (IV) or (V) respectively.

Let G be as in Cases 4 to 7 of Table 2.1. If $d = 2$, then $m = 1$, and so G is as in Case 4 or 6. By [3, Tables 2.2 & 2.3] this action is equivalent to the action of $\mathrm{SL}_2(q)$ on $\mathcal{PG}_1(V)$, and so G is as in Case (III). Hence assume that $d \geq 3$. By Lemmas 2.7.12 and 2.7.13 it follows that $G \leq \mathrm{P\Gamma L}_d(q)$ and $|\Omega| > q^{\frac{1}{2}m(d-m)}$, and so G is as in Case (IX).

Hence we may assume that G is as in Case 8 to 18 of Table 2.1. We begin by considering $G_0 = \mathrm{P}\Omega_d^+(q)$ for certain values of d. If $d \leq 6$, then by [43, p118-119] the action of G is equivalent to another case. If $d = 8$ then G is as in Case (VII). If $d = 2m \geq 10$ then G is as in Case (VIII).

Therefore if $G_0 = \mathrm{P}\Omega_d^+(q)$ then we may assume that $d \geq 10$ and $d \neq 2m$. Hence by Lemmas 2.7.12 and 2.7.13 $G \leq \mathrm{P\Gamma L}_d(q)$ and $|\Omega| > q^{\frac{1}{2}m(d-m)}$. Since G is almost simple, it follows that $d \geq 3$ and so G is as in Case (IX). □

Chapter 3

Numerical Invariants of Primitive Permutation Groups

The work in this section first appeared in [35]. Let G be a primitive non-large-base subgroup of $\mathrm{S}_n = \mathrm{Sym}(\{1, \ldots, n\})$. Emulating Liebeck's work on base size, in [28] Gill, Lodá and Spiga prove the following two theorems.

Theorem 3.0.1 ([28, Theorem 1.3 and Corollaries 1.4 and 1.5])**.** *Let G be a primitive subgroup of S_n. If G is not large base, then*

$$\mathrm{H}(G) < 9 \log n, \quad \mathrm{B}(G) < 9 \log n \quad \textit{and} \quad \mathrm{RC}(G) < 9 \log n + 1.$$

Theorem 3.0.2 ([28, Theorem 1.6])**.** *Let G be a finite primitive group of degree n. Then one of the following holds:*

(i) *There exists an almost simple group A, with socle S, such that G is a subgroup of $A \wr \mathrm{Sym}(r)$ containing S_r, the action of A is one of the following:*

  (a) the action of $\mathrm{Sym}(m)$ on k-subsets of $\{1, ..., m\}$;

  (b) the action of a classical group on a set of subspaces of the natural module, or on a set of pairs of subspaces;

  and the action of the wreath product has the product action of degree $n = s^r$, where s is the degree of the action of A.

(ii) $\mathrm{I}(G) < 7 \log n$.

In Section 3.4, we include bounds on $\mathrm{I}(G)$ for certain families of groups which Gill, Lodá and Spiga proved as part of the proof of the above Theorem. The authors also conjecture that there exists a constant $C > 0$ such that if G is a primitive group of degree n that is not large base, then $\mathrm{I}(G) < C \log n$.

Our main result of the chapter establishes this conjecture.

Theorem 3.0.3. *Let G be a primitive subgroup of S_n. If G is not large base, then*

$$\mathrm{I}(G) < 5 \log n.$$

Let q be a prime power, let $1 \leq m \leq \frac{d}{2}$ and let Ω be the set of m-spaces of $\mathrm{GF}(q)^d$. In addition to the above, in Theorems 3.1.2 and 3.2.1, we find lower bounds on $\mathrm{I}(G, \Omega)$ and $\mathrm{B}(G, \Omega)$ in terms of d and m.

By Lemma 2.3.1(iii) and Theorem 2.2.3, $\mathrm{I}(G) \leq (\mathrm{b}(G) - 1) \log n + 1$ and $\mathrm{b}(G) \leq 9 \log n$. Hence it follows that $\mathrm{I}(G) = O(\log^2 n)$. Therefore Theorem 3.0.3 is not the first bound on $\mathrm{I}(G)$, but it is the first logarithmic bound.

The following shows that for any positive constant c, there are infinitely many examples of primitive groups with $\mathrm{I}(G) > c\mathrm{b}(G)$.

Theorem 3.0.4. *There are infinitely many n for which there exists a primitive group $G \leq \mathrm{S}_n$ such that*

$$\mathrm{I}(G) > \frac{8}{63} \mathrm{b}(G) \log n.$$

It follows immediately from Theorem 3.0.3 and Lemma 2.2.15 that we can tighten the current bounds for the height, maximal size of a minimal base, and relational complexity.

Corollary 3.0.5. *Let G be a primitive subgroup of S_n. If G is not large base, then*

$$\mathrm{RC}(G) < 5 \log n + 1, \quad \mathrm{B}(G) < 5 \log n, \quad \textit{and} \quad \mathrm{H}(G) < 5 \log n.$$

Combining Blaha's greedy base algorithm described in Section 2.4 with Theorem 3.0.3 gives the following corollary.

Corollary 3.0.6. *Let G be a primitive subgroup of S_n which is not large base. Then a greedy algorithm produces a base of size at most $5 \log n$ in polynomial time.*

The chapter is structured as follows. In Section 3.1 we calculate upper and lower bounds on $\mathrm{I}(\mathrm{PGL}_d(q), \Omega)$ in terms of m and d which differ by only a small amount, and then an upper bound on $\mathrm{I}(\mathrm{P\Gamma L}_d(q), \Omega)$ as a function of $|\Omega|$. In the next section we calculate a lower bound on $\mathrm{B}(\mathrm{PGL}_d(q), \Omega)$ as a function of m and d. In Section 3.3 we prove a slight strengthening of Theorem 3.0.3 for almost simple groups. Finally, in Section 3.4 we complete the proof of Theorems 3.0.3 and 3.0.4.

3.1 Bounds on $\mathbf{I}(\mathbf{P}\Gamma\mathbf{L}_d(q))$

Throughout this section we use the following notation.

Notation 3.1.1. Let p be prime, let $f \geq 1$, let $q = p^f$ and let $1 \leq m \leq \frac{d}{2}$. Let $\mathbb{F} = \mathrm{GF}(q)$, let $V = \mathbb{F}^d$, let $\mathbb{F}^*$ be the non-zero elements of $\mathbb{F}$ and let I be the $d \times d$ identity matrix. Let $\Omega = \mathcal{PG}_m(V)$ be the set of all m-dimensional subspaces of V and let $n = |\Omega|$.

We begin by proving the following, which in the case $m = 1$ recovers the lower bounds found by Lodá in [43].

Theorem 3.1.2. *Let* $\mathrm{PGL}_d(q)$ *act on* Ω. *Then*

$$\mathrm{I}(\mathrm{PGL}_d(q)) \leq (m+1)d - 2m + 1,$$

and

$$\mathrm{I}(\mathrm{PGL}_d(q)) \geq \begin{cases} md - m^2 + 1 & \text{if } q = 2, \\ (m+1)d - m^2 & \text{if } q \neq 2. \end{cases}$$

By finding lower bounds on $|\Omega|$ we then prove the following proposition.

Proposition 3.1.3. *Let* $G = \mathrm{P\Gamma L}_d(q)$ *and assume that* $m \leq \frac{d}{2}$. *Then*

$$\mathrm{I}(G, \Omega) \leq \begin{cases} 2(d-1)+1 & \leq 2\log n + 1 & \text{if } m = 1 \text{ and } q = 2, \\ \frac{4}{3}(d-1)\log q + 1 + \log f & \leq \frac{4}{3}\log n + 1 + \log f & \text{if } m = 1 \text{ and } q \geq 3, \\ \frac{d^2}{2} + 1 & \leq 2\log n & \text{if } m = \frac{d}{2} \geq 2 \text{ and } q = 2, \\ 2m(d-m)\log q + \log f & \leq 2\log n + \log f & \text{otherwise.} \end{cases}$$

We divide into three subsections. The first and second subsections are devoted to the upper and lower bounds of Theorem 3.1.2 respectively. In the third we prove Proposition 3.1.3.

3.1.1 Upper bounds as a function of m and d

To prove the upper bound of Theorem 3.1.2 we let $M = M(V)$ be the algebra of all linear maps on V, and consider the action of M on Ω. We begin by introducing subsets of M and then showing that they are subspaces.

Notation 3.1.4. Let $l > 1$ be an integer, let $\Lambda = (\omega_1, \ldots, \omega_l) \in \Omega^l$ and let $\omega_0 = \langle \underline{0} \rangle$. For $0 \leq k \leq l$ let

$$M_k = \{g \in M \mid \omega_i g \leq \omega_i \text{ for } 0 \leq i \leq k\}, \text{ so that } M_0 = M.$$

Lemma 3.1.5. *Let $0 \leq k \leq l-1$. Then $M_{k+1} \leq M_k$.*

Proof. Let $0 \leq i \leq k+1$, let $g, h \in M_{k+1}$, let $v \in \omega_i$ and let $\lambda \in \mathbb{F}$. Then $vg, vh \in \omega_i$, and since ω_i is closed under addition and scalar multiplication it follows that $v(\lambda g) = \lambda(vg) \in \omega_i$ and $v(g+h) = vg + vh \in \omega_i$. Hence $\lambda g, g+h \in M_{k+1}$, and so M_{k+1} is a subspace of M. Since $M_{k+1} \subseteq M_k$, it follows that M_{k+1} is a subspace of M_k. □

For the remainder of this section we make the following assumption.

Assumption 3.1.6. *Let Λ be such that*

$$M_0 > M_1 > \cdots > M_l = \mathbb{F}I$$

with l as large as possible.

We will show that under this assumption l is an upper bound for $\mathrm{I}(\mathrm{PGL}_d(q), \Omega)$, and then by bounding l we prove the upper bound in Theorem 3.1.2.

Lemma 3.1.7. *Let $u = \dim(\omega_1 \cap \omega_2)$. Then there exists a basis $\{e_1, \ldots, e_d\}$ for V, and for $1 \leq k \leq l$ there exist integers a_k such that*

$$m = a_1 \leq \cdots \leq a_l = d, \qquad \langle e_1, \ldots, e_{a_k}\rangle = \langle \omega_1, \ldots, \omega_k \rangle \qquad \textit{and} \qquad \omega_1 \cap \omega_2 = \langle e_1, \ldots e_u \rangle.$$

Proof. Let $W = \langle \omega_1, \ldots, \omega_l \rangle$ and let $r = \dim(W)$. Fix a basis $e_1, \ldots, e_r$ for W which first goes through $\omega_1 \cap \omega_2$, then extends to a basis of ω_1, and then for each $k \geq 2$ extends successively to a basis of $\langle \omega_1, \ldots, \omega_k \rangle$.

For $1 \leq k \leq l$ let $a_k = \dim(\langle \omega_1, \ldots, \omega_k \rangle)$. Hence, by choice of basis, it follows that $\langle \omega_1, \ldots, \omega_k \rangle = \langle e_1, \ldots, e_{a_k} \rangle$. Since $\langle \omega_1, \ldots, \omega_{k-1} \rangle \leq \langle \omega_1, \ldots, \omega_{k-1}, \omega_k \rangle$, it follows that $a_{k-1} \leq a_k$ and so $a_1 \leq a_2 \leq \cdots \leq a_l$.

It follows immediately from the fact that ω_1 is an m-space that $a_1 = m$. If $r < d$ then $T := I + E_{d,d}$ fixes W pointwise and so $T \in M_l \backslash \mathbb{F}I$, contradicting assumption 3.1.6. Hence $a_l = r = d$. □

Since $\omega_0 = \langle \underline{0} \rangle$, we may let $a_0 = 0$. From now on we identify M with the set of $d \times d$ matrices, and $\mathrm{GL}_d(q)$ with the set of invertible $d \times d$ matrices, over $\mathbb{F}$ with respect to this basis.

In the following Lemma we prove that l is an upper bound on $\mathrm{I}(\mathrm{PGL}_d(q), \Omega)$. In addition, for use in later sections, we compare the action of $\mathrm{PGL}_d(q)$ and $\mathrm{GL}_d(q)$ on sequences of points in Ω. As in Section 2.3, for G a group acting on Ω and $(\omega_1, \ldots, \omega_k) \in \Omega^k$, we let $G^{(i)} = G_{\omega_1, \ldots, \omega_i}$ for $0 \leq i \leq k$, and so $G^{(0)} = G$.

Lemma 3.1.8. *Let $P = \mathrm{PGL}_d(q)$ and $G = \mathrm{GL}_d(q)$ act on Ω, and let $Z = \mathrm{Z}(G) = \mathbb{F}^*I$. Then the following hold.*

(i) *Λ is a minimal base for P if and only if $G_\Lambda = Z$ and $G_{\Lambda\setminus\{\lambda\}} \neq Z$ for all $\lambda \in \Lambda$.*

(ii) *$\Lambda \in \Omega^k$ is an irredundant base for P if and only if*

$$G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(k)} = Z.$$

(iii) *$\mathrm{I}(P, \Omega) \leq l$.*

Proof. (i) This case follows since $P_\Lambda = G_\Lambda/Z$ and $P_{\Lambda\setminus\{\lambda\}} = G_{\Lambda\setminus\{\lambda\}}/Z$ for $\lambda \in \Lambda$.

(ii) By (i) $G^{(k)} = Z$ if and only if $P^{(k)} = 1$. If $P^{(i)} > P^{(i+1)}$, then $G^{(i)} > G^{(i+1)}$. Also, if $G^{(i)} > G^{(i+1)} > Z$, then it follows that $P^{(i)} > P^{(i+1)}$.

(iii) Let $\mathrm{I}(P, \Omega) = k$ with corresponding base $(\omega_1, \ldots, \omega_k) \in \Omega^k$. Then by (ii)

$$G > G_{\omega_1} > G_{\omega_1,\omega_2} > \cdots > G_{\omega_1,\ldots,\omega_k} = Z.$$

Since, as sets $G \subseteq M$, it follows that

$$M > M_1 > M_2 > \cdots > M_k \geq \mathbb{F}I.$$

Now since l is chosen to be maximal, we deduce that $l \geq k$. □

By the previous lemma, if we can prove that $l \leq (m+1)d - 2m + 1$, then the upper bound in Theorem 3.1.2 will follow. We now introduce some definitions and lemmas which we shall use to prove this bound.

Definition 3.1.9. For $0 \leq k \leq l-1$, let

$$b_k = a_{k+1} - a_k \quad \text{and} \quad f_k = \dim(M_k) - \dim(M_{k+1}).$$

We first bound the values of b_k.

Lemma 3.1.10. (i) *$0 \leq b_k \leq m$ for all k.*

(ii) *$b_0 = m$ and $b_1 \neq 0$.*

(iii) *For all k there exist $v_1, \ldots v_{m-b_k} \in \langle \omega_1 \ldots, \omega_k \rangle = \langle e_1, \ldots, e_{a_k} \rangle$ such that $\omega_{k+1} = \langle v_1, \ldots v_{m-b_k}, e_{a_k+1}, \ldots, e_{a_k+b_k} \rangle$.*

Proof. (i) Since $a_k \leq a_{k+1}$ by Lemma 3.1.7, it follows that $0 \leq a_{k+1} - a_k$. In addition

$$a_{k+1} = \dim(\langle \omega_1, \ldots, \omega_k, \omega_{k+1} \rangle) \leq \dim(\langle \omega_1, \ldots, \omega_k \rangle) + \dim(\langle \omega_{k+1} \rangle) = a_k + m,$$

and so $a_{k+1} - a_k \leq m$. Hence $0 \leq b_k \leq m$.

(ii) From $a_0 = 0$ and $a_1 = m$, it follows that $b_0 = m$.

Assume, by way of a contradiction, that $b_1 = 0$. Then $b_1 = a_2 - a_1 = 0$, and so $a_2 = a_1 = m$ and $\langle \omega_1, \omega_2 \rangle = \langle e_1, \ldots, e_{a_2} \rangle = \langle e_1, \ldots, e_m \rangle$. Since ω_1 and ω_2 are both m-spaces it follows that $\omega_1 = \omega_2$ and so $M_1 = M_2$, contradicting Assumption 3.1.6.

(iii) This is an immediate consequence of the choice of basis. □

We now introduce lemmas which bound f_k in terms of b_k.

Lemma 3.1.11. (i) *The dimension of M_1 is $d^2 - m(d-m)$, and so $f_0 = m(d-m)$; and*

(ii) $f_1 = b_1(d - b_1)$.

Proof. (i) It follows from $\omega_1 = \langle e_1, \ldots, e_m \rangle$, that $g = (g_{ij}) \in M_1$ if and only if $e_i g \in \omega_1$ for $1 \leq i \leq m$. Equivalently, $g_{ij} = 0$ for $1 \leq i \leq m$, $m+1 \leq j \leq d$. Hence $\dim(M_1) = d^2 - m(d-m)$, and the final claim follows since $\dim(M_0) = d^2$.

(ii) By Lemma 3.1.7, $\omega_1 \cap \omega_2 = \langle e_1, \ldots, e_{m-b_1} \rangle$. Hence the subspace M_2 contains all matrices of shape

$$\begin{pmatrix} x_1 & 0 & 0 & 0 \\ x_2 & x_3 & 0 & 0 \\ x_4 & 0 & x_5 & 0 \\ y_1 & y_2 & y_3 & y_4 \end{pmatrix}$$

where x_1, x_3 and x_5 are square with $m - b_1$, b_1 and b_1 rows respectively. Hence

$$\begin{aligned} \dim(M_2) &= \sum_{i=1}^{5} \dim(x_i) + \sum_{i=1}^{4} \dim(y_i) \\ &= \dim(x_1) + 2\dim(x_2) + 2\dim(x_3) + d(d - m - b_1) \\ &= (m - b_1)^2 + 2b_1(m - b_1) + 2b_1^2 + d(d - m - b_1) \\ &= d^2 - m(d-m) - b_1(d - b_1), \end{aligned}$$

and the result follows from Part (i). □

To bound f_k for the remaining values of k we introduce the following definition and two lemmas.

Definition 3.1.12. For $0 \leq k \leq l$ we define two subspaces of M_k, namely

$$\begin{aligned} X_k &= \{g \in M_k \mid e_i g = \underline{0} \text{ for } a_k + 1 \leq i \leq d\} \text{ and} \\ Y_k &= \{g \in M \mid e_i g = \underline{0} \text{ for } 1 \leq i \leq a_k\}. \end{aligned}$$

Lemma 3.1.13. *For $0 \leq k \leq l$*

$$M_k = X_k \oplus Y_k \quad \textit{and} \quad \dim(Y_k) = d(d - a_k).$$

Proof. Let $g = (g_{ij}) \in M$. If $g \in X_k \cap Y_k$, then $e_i g = \underline{0}$ for $1 \leq i \leq d$, and so $X_k \cap Y_k = \{0_M\}$.

Let $g, h \in X_k$, let $a_k + 1 \leq i \leq d$ and let $\lambda \in \mathbb{F}$ then

$$e_i(g + h) = e_i g + e_i h = \underline{0} + \underline{0} = \underline{0} \quad \text{and} \quad e_i(\lambda g) = \lambda e_i g = \lambda \underline{0} = \underline{0}.$$

Hence $g + h, \lambda g \in X_k$ and so $X_k \leq M$. Similarly $Y \leq M$. We now show that $\omega_j Y_k \leq \omega_j$ for $1 \leq j \leq k$, from which it will follow that $Y_k \leq M_k$. Let $1 \leq j \leq k$, let $u \in \omega_j$ and let $y \in Y_k$. From $\langle \omega_1, \dots, \omega_j \rangle = \langle e_1, \dots, e_{a_j} \rangle$, it follows that $u_i = 0$ for $a_j + 1 \leq i \leq d$. Hence

$$\begin{aligned}
(uy)_t &= \sum_{i=1}^{d} u_i y_{it} \\
&= \sum_{i=1}^{d} u_i e_i y e_t^T \\
&= \sum_{i=1}^{a_j} u_i e_i y e_t^T + \sum_{i=a_j+1}^{d} u_i e_i y e_t^T \\
&= \sum_{i=1}^{a_j} u_i \underline{0} e_t^T + \sum_{i=a_j+1}^{d} 0 e_i y e_t^T \\
&= 0
\end{aligned}$$

Therefore $uy = \underline{0} \in \omega_i$, and so $\omega_i y \leq \omega_i$. Thus $Y_k \leq M_k$, and so $X_k \oplus Y_k \leq M_k$.

We now show that $M_k \leq X_k \oplus Y_k$. If $g \in M_k$, then there exists $x = (x_{ij}), y = (y_{ij}) \in M$ satisfying the following.

$$x_{ij} = \begin{cases} g_{ij} & \text{if } i \leq a_k \\ 0 & \text{if } i \geq a_k + 1 \end{cases} \qquad y_{ij} = \begin{cases} 0 & \text{if } i \leq a_k \\ g_{ij} & \text{if } i \geq a_k + 1 \end{cases}$$

Then $g = x + y$ and $x \in X_k$, $y \in Y_k$. Hence $M_k \leq X_k \oplus Y_k$ and so $M_k = X_k \oplus Y_k$.

Since $g \in Y_k$ if and only if $g_{ij} = 0$ for $i \leq a_k$, it follows that $\dim(Y_k) = d(d - a_k)$. □

Lemma 3.1.14. $\dim(X_{k+1}) - \dim(X_k) \leq b_k m$.

Proof. By Lemma 3.1.13, we can rephrase X_k as in Definition 3.1.12 as follows.

$$X_k = \left\{ g \in M \;\middle|\; g_{ij} = \begin{cases} h_{ij} & 1 \leq i \leq a_k, \\ 0 & \text{otherwise,} \end{cases} \text{ for some } h \in M_k \right\}.$$

Thus $M_{k+1} \leq M_k$ and $a_{k+1} = a_k + b_k$ imply the following

$$\begin{aligned}
X_{k+1} &= \left\{ g \in M \;\middle|\; g_{ij} = \begin{cases} h_{ij} & 1 \leq i \leq a_k + b_k, \\ 0 & \text{otherwise,} \end{cases} \text{for some } h \in M_{k+1} \right\} \\
&\leq \left\{ g \in M \;\middle|\; g_{ij} = \begin{cases} f_{ij} & 1 \leq i \leq a_k, \\ h_{ij} & a_k + 1 \leq i \leq a_k + b_k, \\ 0 & \text{otherwise,} \end{cases} \text{for some } f \in M_k, \;\; h \in M_{k+1} \right\} \\
&:= \overline{X_{k+1}}.
\end{aligned}$$

Therefore $X_k \leq \overline{X_{k+1}}$, and by identifying X_k with $\underline{0}$ in $\overline{X_{k+1}}/X_k$ it follows that

$$\begin{aligned}
\overline{X_{k+1}}/X_k &\cong \left\{ g \in M \;\middle|\; g_{ij} = \begin{cases} h_{ij} & a_k + 1 \leq i \leq a_k + b_k, \\ 0 & \text{otherwise,} \end{cases} \text{for some } h \in M_{k+1} \right\} \\
&= \left\{ g \in M \;\middle|\; e_i g = \begin{cases} e_i h & a_k + 1 \leq i \leq a_k + b_k, \\ 0 & \text{otherwise,} \end{cases} \text{for some } h \in M_{k+1} \right\} \\
&\leq \left\{ g \in M \;\middle|\; e_i g = \begin{cases} e_i h_i & a_k + 1 \leq i \leq a_k + b_k, \\ 0 & \text{otherwise,} \end{cases} \text{for some } h_{a_k+1}, \ldots, h_{a_k+b_k} \in M_{k+1} \right\}.
\end{aligned}$$

The final space above is isomorphic to the external direct sum $\bigoplus_{i=a_k+1}^{a_k+b_k} \langle e_i M_{k+1} \rangle$. Now $\omega_{k+1} = \langle v_1, \ldots, v_{m-b_k}, e_{a_k+1}, \ldots, e_{a_k+b_k} \rangle$ for some $v_1, \ldots, v_{m-b_k} \in \langle \omega_1, \ldots, \omega_k \rangle$ by Lemma 3.1.10(iii). Hence $e_i M_{k+1} \leq \omega_{k+1}$ for $a_k + 1 \leq i \leq a_k + b_k$ and so

$$\bigoplus_{i=a_k+1}^{a_k+b_k} \langle e_i M_{k+1} \rangle \leq \bigoplus_{i=a_k+1}^{a_k+b_k} \omega_{k+1}.$$

Therefore

$$\begin{aligned}
\dim(X_{k+1}) - \dim(X_k) &\leq \dim(\overline{X_{k+1}}) - \dim(X_k) \\
&= \dim(\overline{X_{k+1}}/X_k) \\
&\leq \dim\left(\bigoplus_{i=a_k+1}^{a_k+b_k} \omega_{k+1} \right) \\
&= \sum_{i=a_k+1}^{a_k+b_k} \dim(\omega_{k+1}) \\
&= b_k m.
\end{aligned}$$

□

Lemma 3.1.15. *Let $k \neq 1$. Then $f_k \geq \max\{1, b_k(d-m)\}$.*

Proof. If $k = 0$, then $b_0 = m$ and $f_0 = m(d-m)$ by Lemmas 3.1.10(ii) and 3.1.11(i). Hence the result holds for $k = 0$.

Next assume that $k \geq 2$. Our assumption that $M_k > M_{k+1}$ implies that $f_k \geq 1$, so we may assume that $b_k \geq 1$. Then

$$\begin{aligned} f_k &= \dim(M_k) - \dim(M_{k+1}) \\ &= \big(\dim(X_k) + \dim(Y_k)\big) - \big(\dim(X_{k+1}) + \dim(Y_{k+1})\big) \quad \text{by Lemma 3.1.13} \\ &= \dim(X_k) - \dim(X_{k+1}) + d(d - a_k) - d(d - a_{k+1}) \qquad \text{by Lemma 3.1.13} \\ &= \dim(X_k) - \dim(X_{k+1}) + d(a_{k+1} - a_k) \\ &= \dim(X_k) - \dim(X_{k+1}) + b_k d \\ &\geq -b_k m + b_k d \qquad \text{by Lemma 3.1.14} \\ &= b_k(d - m). \end{aligned}$$

□

Using the bounds on f_k in Lemmas 3.1.11 and 3.1.15, we can now prove the upper bound of Theorem 3.1.2.

Proof of upper bound of Theorem 3.1.2. We shall show that $l \leq (m+1)d - 2m + 1$, hence by Lemma 3.1.8(iii) the result will follow. We begin by introducing and bounding some variables which encapsulate the restrictions on l.

For $0 \leq b \leq m$, let

$$C_b = \big\{k \in \{0, \dots, l-1\} \bigm| b_k = b\big\}$$

and let $c_b = |C_b|$. Then

$$l = \sum_{b=0}^{m} c_b. \tag{3.1}$$

Since $a_l = d$ and $a_0 = 0$ it follows that

$$d = a_l - a_0 = \sum_{k=0}^{l-1}(a_{k+1} - a_k) = \sum_{k=0}^{l-1} b_k = \sum_{b=0}^{m}\sum_{k \in C_b} b = \sum_{b=0}^{m} bc_b = \sum_{b=1}^{m} bc_b. \tag{3.2}$$

By Lemma 3.1.10(ii) $b_0 = m$ and $b_1 \geq 1$. Hence $0 \in C_m$ and $1 \in C_{b_1} \neq C_0$. Therefore

$$c_{b_1} \geq 1 \quad \text{and} \quad c_m \geq 1 + \delta_{mb_1}. \tag{3.3}$$

Recall by Lemmas 3.1.11 and 3.1.15 that

$$f_1 = b_1(d - b_1) \quad \text{and} \quad f_k \geq \max\{1, b_k(d-m)\} \text{ for } k \neq 1.$$

Hence

$$f_1 = b_1(m - b_1) + b_1(d - m) \quad \text{and} \quad f_k \geq \begin{cases} 1 & \text{if } k \in C_0, \\ b_k(d-m) & \text{otherwise.} \end{cases} \tag{3.4}$$

Therefore

$$\begin{aligned}
d^2-1 &= \dim(M_0)-\dim(M_l) \qquad \text{by Assumption 3.1.6}\\
&= \sum_{k=0}^{l-1}\Big(\dim(M_k)-\dim(M_{k+1})\Big)\\
&= \sum_{k=0}^{l-1} f_k\\
&= \sum_{k\in C_0} f_k + \sum_{k\in C_{b_1}} f_k + \sum_{k\notin C_0\cup C_{b_1}} f_k\\
&= \sum_{k\in C_0} f_k + f_1 + \sum_{k\in C_{b_1}\setminus\{1\}} f_k + \sum_{k\notin C_0\cup C_{b_1}} f_k\\
&\geq \sum_{k\in C_0} 1 + b_1(m-b_1) + b_1(d-m) + \sum_{k\in C_{b_1}\setminus\{1\}} b_1(d-m) + \sum_{k\notin C_0\cup C_{b_1}} b_k(d-m) \qquad \text{by (3.4)}\\
&= c_0 + b_1(m-b_1) + \sum_{k\in C_{b_1}} b_1(d-m) + \sum_{k\notin C_0\cup C_{b_1}} b_k(d-m)\\
&= c_0 + b_1(m-b_1) + \sum_{k\notin C_0} b_k(d-m)\\
&= c_0 + b_1(m-b_1) + (d-m)\sum_{k\notin C_0} b_k\\
&= c_0 + b_1(m-b_1) + (d-m)\sum_{b=1}^{m} bc_b\\
&= c_0 + b_1(m-b_1) + (d-m)d \qquad \text{by (3.2).}
\end{aligned}$$

By rearranging we find that

$$c_0 \leq md - b_1(m-b_1) - 1. \tag{3.5}$$

We bound I(G) by maximizing $l=\sum_{b=0}^{m} c_b$ subject only to Equations (3.2), (3.3) and (3.5). By (3.2) an upper bound on $\sum_{b=0}^{m} c_b$ is given by maximizing c_0, maximizing c_b for b small and minimizing c_b for b large. Hence we substitute $c_0 = md - b_1(m-b_1) - 1$ and $c_b = 0$ for $b \notin \{0,1,b_1,m\}$; and we maximise c_1 and minimise c_m subject to (3.3).

We now show that $|C_1 \cup C_{b_1} \cup C_m| = 2 + d - m - b_1$, for all possible values of m and b_1. First let $m=1$. Then it follows by Lemma 3.1.10(ii) that $b_1 = m$. Hence $c_1 = d$ by (3.2) and so

$$|C_1 \cup C_{b_1} \cup C_m| = |C_1| = d = 2 + d - 1 - 1 = 2 + d - m - b_1.$$

Now let $m \geq 2$. Then there are three possibilities for b_1. If $b_1 = m$, then to minimise c_m

subject to (3.3) let $c_m = 2$. Therefore (3.2) yields $c_1 = d - 2m$, and so

$$|C_1 \cup C_{b_1} \cup C_m| = |C_1 \cup C_m| = d - 2m + 2 = 2 + d - m - m = 2 + d - m - b_1.$$

If $b_1 = 1$, then let $c_m = 1$, and so (3.2) yields $c_1 = d - m$. Hence

$$|C_1 \cup C_{b_1} \cup C_m| = |C_1 \cup C_m| = d - m + 1 = 2 + d - m - 1 = 2 + d - m - b_1.$$

Otherwise $1 < b_1 < m$ are distinct, and so to minimise c_m and c_{b_1} subject to (3.3), we substitute $c_m = c_{b_1} = 1$. Hence (3.2) yields $c_1 = d - m - b_1$, and so

$$|C_1 \cup C_{b_1} \cup C_m| = d - m - b_1 + 1 + 1 = 2 + d - m - b_1.$$

Hence

$$\begin{aligned}\sum_{b=0}^{m} c_b &= c_0 + |C_1 \cup C_{b_1} \cup C_m| \\ &= md - b_1(m - b_1) - 1 + 2 + d - m - b_1 \\ &= (m+1)d - m + 1 - b_1(m - b_1 + 1).\end{aligned}$$

Hence $\sum_{b=0}^{m} c_b$ is maximal when $f(b_1) := b_1(m - b_1 + 1)$ is minimal subject to $1 \leq b_1 \leq m$. Since $f(b_1)$ is a negative quadratic with roots $b_1 = 0$ and $b_1 = m + 1$, the minimal value of $f(b_1)$ over $1 \leq b_1 \leq m$ is $f(1) = f(m) = m$. Therefore

$$\sum_{b=0}^{m} c_b \leq (m+1)d - 2m + 1,$$

and result now follows from (3.1). □

3.1.2 Lower bounds as a function of m and d

In this subsection we prove the lower bounds in Theorem 3.1.2. We begin with some notation.

Notation 3.1.16. Let $g^{(i)}$ be a $d \times d$ matrix with entries in $\{0, *, \lambda, \mu, \lambda \pm \mu\}$. Then we say that $g^{(i)}$ is a representative matrix for the group $G^{(i)}$ defined to be the group of matrices $h \in \mathrm{GL}_d(q)$ satisfying the following properties.

(i) If $g^{(i)}_{jk} = 0$, then $h_{jk} = 0$.

(ii) If $g^{(i)}_{jk} = \lambda = g^{(i)}_{lm}$ or $g^{(i)}_{jk} = \mu = g^{(i)}_{lm}$, then $h_{jk} = h_{lm}$.

(iii) If $g^{(i)}_{jk} = \lambda$, $g^{(i)}_{lm} = \mu$ and $g^{(i)}_{no} = \lambda \pm \mu$, then $h_{no} = h_{jk} \pm h_{lm}$.

For example, let

$$g^{(1)} = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}, \qquad g^{(2)} = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \qquad \text{and} \qquad g^{(3)} = \begin{pmatrix} \lambda & 0 & 0 \\ \mu & \lambda+\mu & 0 \\ * & * & * \end{pmatrix}.$$

Then $G^{(1)}$ the group of 3×3 upper triangular matrices, and $G^{(2)}$ is $\mathbb{F}^* I = \mathrm{Z}(\mathrm{GL}_3(q))$ and $G^{(3)}$ is the pointwise stabilizer in $\mathrm{GL}_d(q)$ of $\langle e_1 \rangle$ and $\langle e_1 + e_2 \rangle$.

To prove the lower bound of Theorem 3.1.2 we construct Λ a sequence of m-spaces, and show that Λ is an irredundant base for $\mathrm{PGL}_d(q)$. In the following example we give Λ as described above for $\mathrm{PGL}_5(q)$ acting on 2-spaces. This will illustrate the notation and methods used in the proof of the lower bound.

Recall that for $G \leq \mathrm{Sym}(\Omega)$ and for $\Lambda = (\omega_1, \ldots, \omega_l) \in \Omega^l$, we let $G^{(i)} = G_{\omega_1,\ldots,\omega_i}$ for $1 \leq i \leq l$.

Example 3.1.17. Let $\mathbb{F} = \mathrm{GF}(q)$, and let $G = \mathrm{GL}_5(q)$ act on $\Omega = \mathcal{PG}_2(\mathbb{F}^5)$. We construct $\Lambda = (\omega_1, \ldots, \omega_{11}) \in \Omega^{11}$ and show that if $q = 2$ then

$$G^{(0)} > G^{(1)} > \cdots > G^{(7)} = \mathbb{F}^* I,$$

and if $q > 2$ then

$$G^{(0)} > G^{(1)} > \cdots > G^{(11)} = \mathbb{F}^* I.$$

Hence by Lemma 3.1.8(ii), $\mathrm{I}(\mathrm{PGL}_5(2), \Omega)$ is bounded below by 7; and $\mathrm{I}(\mathrm{PGL}_5(q), \Omega)$ is bounded below by 11 for $q > 2$.

Let $1 \leq k \leq 11$, and let

$$r_k = \left\lfloor \frac{k-2}{2} \right\rfloor + 3, \qquad s_k = 2 - (k - 2 \bmod 2), \qquad \text{and } \ t_k = k - 6.$$

Hence

$$(r_4, s_4) = (4, 2), \quad (r_5, s_5) = (4, 1), \quad (r_6, s_6) = (5, 2) \quad \text{and} \quad (r_7, s_7) = (5, 1)$$

and

$$t_8 = 2, \quad t_9 = 3, \quad t_{10} = 4 \quad \text{and} \quad t_{11} = 5.$$

For $1 \leq k \leq 11$ let

$$W_k = \begin{cases} \{e_i \mid i \in \{1,2,3\} \backslash \{4-k\}\} & \text{for } 1 \leq k \leq 3, \\ \{e_i \mid i \in \{1,2,r_k\} \backslash \{s_k\}\} & \text{for } 4 \leq k \leq 7 \\ \{e_1 + e_{t_k}, e_i \mid i \in \{2,3\} \backslash \{t_k\}\} & \text{for } 8 \leq k \leq 9, \\ \{e_1 + e_{t_k}, e_i \mid i \in \{2\}\} & \text{for } 10 \leq k \leq 11, \end{cases}$$

and so each W_k is as follows

$$\begin{array}{ll} W_1 = \{e_1, e_2.e_3\} \backslash \{e_3\} = \{e_1, e_2\} & W_2 = \{e_1, e_2, e_3\} \backslash \{e_2\} = \{e_1, e_3\} \\ W_3 = \{e_1, e_2, e_3\} \backslash \{e_1\} = \{e_2, e_3\} & W_4 = \{e_1, e_2, e_4\} \backslash \{e_2\} = \{e_1, e_4\} \\ W_5 = \{e_1, e_2, e_4\} \backslash \{e_1\} = \{e_2, e_4\} & W_6 = \{e_1, e_2, e_5\} \backslash \{e_2\} = \{e_1, e_5\} \\ W_7 = \{e_1, e_2, e_5\} \backslash \{e_1\} = \{e_2, e_5\} & W_8 = \{e_1 + e_2, e_2, e_3\} \backslash \{e_2\} = \{e_1 + e_2, e_3\} \\ W_9 = \{e_1 + e_3, e_2, e_3\} \backslash \{e_3\} = \{e_1 + e_3, e_2\} & W_{10} = \{e_1 + e_4, e_2\} \\ W_{11} = \{e_1 + e_5, e_2\}. & \end{array}$$

For $1 \leq k \leq 11$, let $\omega_k = \langle W_k \rangle \in \Omega$, let $\Lambda = (\omega_1, \ldots, \omega_{11})$ and let $g^{(k)}$ be a representative element of $G^{(k)}$. Hence we have the following.

$$g^{(0)} = \begin{pmatrix} \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix} \quad g^{(1)} = \begin{pmatrix} \ast & \ast & 0 & 0 & 0 \\ \ast & \ast & 0 & 0 & 0 \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix} \quad g^{(2)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ \ast & \ast & 0 & 0 & 0 \\ \ast & 0 & \ast & 0 & 0 \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix}$$

$$g^{(3)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ 0 & \ast & 0 & 0 & 0 \\ 0 & 0 & \ast & 0 & 0 \\ \ast & \ast & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix} \quad g^{(4)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ 0 & \ast & 0 & 0 & 0 \\ 0 & 0 & \ast & 0 & 0 \\ \ast & 0 & 0 & \ast & 0 \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix} \quad g^{(5)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ 0 & \ast & 0 & 0 & 0 \\ 0 & 0 & \ast & 0 & 0 \\ 0 & 0 & 0 & \ast & 0 \\ \ast & \ast & \ast & \ast & \ast \end{pmatrix}$$

$$g^{(6)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ 0 & \ast & 0 & 0 & 0 \\ 0 & 0 & \ast & 0 & 0 \\ 0 & 0 & 0 & \ast & 0 \\ \ast & 0 & 0 & 0 & \ast \end{pmatrix} \quad g^{(7)} = \begin{pmatrix} \ast & 0 & 0 & 0 & 0 \\ 0 & \ast & 0 & 0 & 0 \\ 0 & 0 & \ast & 0 & 0 \\ 0 & 0 & 0 & \ast & 0 \\ 0 & 0 & 0 & 0 & \ast \end{pmatrix}$$

Hence for $1 \leq k \leq 7$, we see by the above that $G^{(k-1)} > G^{(k)}$. In addition, if $q = 2$, then $G^{(7)} = \mathbb{F}^* I$ and so $\mathrm{I}(\mathrm{PGL}_5(2)) \geq 7$.

Next assume that $q > 2$. Then we have the following.

$$g^{(8)} = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & * & 0 & 0 \\ 0 & 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 & * \end{pmatrix} \quad g^{(9)} = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 & * \end{pmatrix} \quad g^{(10)} = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & * \end{pmatrix}$$

$$g^{(11)} = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}$$

Therefore $G^{(k-1)} > G^{(k)}$ for $1 \leq k \leq 11$ and $G^{(11)} = \mathbb{F}^* I$, and so $\mathrm{I}(\mathrm{PGL}_5(q)) \geq 11$. △

Proof of lower bound of Theorem 3.1.2. Recall that we let $q = p^f$ be a prime power, let $\mathbb{F} = \mathrm{GF}(q)$, let $d \geq 2$, let $V = \mathbb{F}^d$, and let $G = \mathrm{GL}_d(q)$ act on $\Omega = \mathcal{PG}_m(V)$. Here we construct $\Lambda = (\omega_1, \ldots, \omega_l) \in \Omega^l$ with

$$G^{(0)} > G^{(1)} > \cdots > G^{(l)} = \mathbb{F}^* I.$$

From which it will follow by Lemma 3.1.8(ii) that Λ is an irredundant base for the action of $\mathrm{PGL}_d(q)$ on Ω, and so $\mathrm{I}(\mathrm{PGL}_d(q), \Omega) \geq l$.

Let $1 \leq k \leq md - m^2 + d$, and let

$$r_k = \left\lfloor \frac{k-2}{m} \right\rfloor + m + 1, \qquad s_k = m - \big((k-2) \bmod m\big), \qquad \text{and} \qquad t_k = k - md + m^2.$$

Hence if $m + 2 \leq k \leq md - m^2 + 1$, then

$$m + 2 \leq r_k \leq d \quad \text{and} \quad 1 \leq s_k \leq m. \tag{3.6}$$

Whilst $t_k \leq d$ for all k, and

$$2 \leq t_k \leq m + 1 \quad \text{if and only if} \quad md - m^2 + 2 \leq k \leq md - m^2 + m + 1.$$

Hence the following are well defined sets of m linearly independent vectors of V.

$$W_k = \begin{cases} \big\{e_i \mid i \in \{1, \ldots, m+1\} \backslash \{m + 2 - k\}\big\} & \text{for } 1 \leq k \leq m+1, \\ \big\{e_i \mid i \in \{1, \ldots, m, r_k\} \backslash \{s_k\}\big\} & \text{for } m + 2 \leq k \leq md - m^2 + 1, \\ \big\{e_1 + e_{t_k}, e_i \mid i \in \{2, \ldots, m+1\} \backslash \{t_k\}\big\} & \text{for } md - m^2 + 2 \leq k \leq md - m^2 + m + 1, \\ \big\{e_1 + e_{t_k}, e_i \mid i \in \{2, \ldots, m\}\big\} & \text{for } md - m^2 + m + 2 \leq k \leq md - m^2 + d. \end{cases}$$

For $1 \leq k \leq md - m^2 + d$, let $\omega_k = \langle W_k \rangle \in \Omega$ and let $G^{(k)} = G_{\omega_1,\ldots,\omega_k}$. For $1 \leq x, y \leq d$, let $T(x, y)$ be the matrix $I + E_{x,y}$, and let $\mathrm{Supp}_x(W_k)$ be the set of vectors in W_k which are non-zero in position x. Then $T(x, y) \in G$ unless $q = 2$ and $x = y$. Recall that

$$e_i T(x, y) = \begin{cases} e_x + e_y & \text{if } i = x, \\ e_i & \text{otherwise.} \end{cases}$$

Hence if a vector v is zero in position x, then $vT(x, y) = v$. Therefore $\omega_k T(x, y) = \omega_k$ if and only if $\mathrm{Supp}_x(W_k)T(x, y) \subseteq \omega_k$. In particular, if $\mathrm{Supp}_x(W_k) = \emptyset$, then
$\omega_k T(x, y) = \omega_k$.

Since G is irreducible it follows that $G > G^{(1)}$. Let $k \in \{2, \ldots, md - m^2 + 1\}$ and let $j \leq k$. We shall show that there exist $1 \leq x, y \leq d$ such that $T(x, y) \in G$ satisfies $\omega_j T(x, y) = \omega_j$ for all $j < k$, and $\omega_k T(x, y) \neq \omega_k$. Hence $T(x, y) \in G^{(k-1)} \backslash G^{(k)}$, and so $G^{(k-1)} > G^{(k)}$.

First let $k \in \{2, \ldots, m+1\}$, and let $T = T(m+1, m+2-k)$. Then $\mathrm{Supp}_{m+1}(W_1) = \emptyset$, and for $2 \leq j \leq k$

$$\mathrm{Supp}_{m+1}(W_j)T = \{e_{m+1}\}T = \{e_{m+1} + e_{m+2-k}\}.$$

Hence $\mathrm{Supp}_{m+1}(W_j)T \subseteq \omega_j$ if and only if $j < k$. Therefore $\omega_j T = \omega_j$ for $j < k$, and $\omega_k T \neq \omega_k$.

Next consider $k \in \{m + 2, \ldots, md - m^2 + 1\}$. Hence (3.6) holds, and so we may let $T = T(r_k, s_k)$. If $j \leq m + 1$ or if $r_j \neq r_k$, then $\mathrm{Supp}_{r_k}(W_j) = \emptyset$ and so $\omega_j T = \omega_j$. Therefore assume that $j \geq m + 2$ and $r_j = r_k$. Then

$$\mathrm{Supp}_{r_k}(W_j)T = \{e_{r_k}\}T = \{e_{r_k} + e_{s_k}\}.$$

Since $(r_j, s_j) = (r_k, s_k)$ if and only if $j = k$, it follows that $\mathrm{Supp}_{r_k}(W_j)T \subseteq \omega_j$ if and only if $j < k$. Therefore $\omega_j T = \omega_j$ for $j < k$, and $\omega_k T \neq \omega_k$. Hence $G^{(k-1)} > G^{(k)}$ for $1 \leq k \leq md - m^2 + 1$, and so if $q = 2$ then the result follows.

Hence it remains to consider $q > 2$ and $md - m^2 + 2 \leq k$. Let $T = T(t_k, t_k)$ and let

$u \in \{e_i, e_1 + e_i \mid 1 \leq i \leq d\}$. Then

$$uT = \begin{cases} e_1 + 2e_{t_k} & \text{if } u = e_1 + e_{t_k}, \\ 2u & \text{if } u = e_{t_k}, \\ u & \text{otherwise.} \end{cases} \tag{3.7}$$

If $1 \leq j \leq md - m^2 + 1$ then $W_j \subseteq \{e_1, \ldots, e_d\}$, and if $md - m^2 + 1 < j < k$ then $W_j \subseteq \{e_1 + e_{t_j}, \ldots, e_d\}$ with $t_j < t_k$. Hence if $j < k$, then $\mathrm{Supp}_{t_k}(W_j)T \subseteq \omega_j$ by (3.7), and so $\omega_j T = \omega_j$. Since $e_1 + e_{t_k} \in \omega_k$ and $e_1 + 2e_{t_k} \notin \omega_k$ it follows that $\omega_k T(t_k, t_k) \neq \omega_k$. Hence $G^{(k-1)} > G^{(k)}$ for $1 \leq k \leq md - m^2 + d$, and so the result follows. □

3.1.3 Upper bounds as a function of $|\Omega|$

In this subsection we prove Proposition 3.1.3, which bounds $\mathrm{I}(\mathrm{P\Gamma L}_d(q), \Omega)$ as a function of $n = |\Omega|$. We begin by bounding the size of $\Omega = \mathcal{PG}_m(\mathbb{F}^d)$.

Lemma 3.1.18. *Let $n(d, m, q) = |\mathcal{PG}_m(\mathbb{F}^d)|$. Then*

$$\log|\Omega| = \log\big(n(d,m,q)\big) > \begin{cases} \frac{d^2}{4} + \frac{1}{2} & \text{if } q = 2 \text{ and } m = \frac{d}{2} \geq 2, \\ m(d-m)\log q & \text{for all } m \text{ and } q. \end{cases}$$

Proof. The second bound holds by [43, Lemma 4.2.8], so let $q = 2$ and $m \geq 2$. The statement of the result is then equivalent to $n(2m, m, 2) > 2^{m^2 + \frac{1}{2}}$.

We now induct on m. By Lemma 2.7.2

$$n(4,2,2) = \frac{(2^4-1)(2^3-1)}{(2^2-1)(2-1)} = 35 > 2^{2^2+\frac{1}{2}},$$

and so the result holds for $m = 2$. Again by Lemma 2.7.2

$$\begin{aligned} n(2m, m, 2) &= \frac{(2^{2m}-1)(2^{2m-1}-1)(2^{2m-2}-1)\cdots(2^{m+1}-1)}{(2^m-1)(2^{m-1}-1)(2^{m-2}-1)\cdots(2-1)} \\ &= \frac{(2^{2m}-1)(2^{2m-1}-1)}{(2^m-1)^2} \cdot \frac{(2^{2m-2}-1)\cdots(2^{m+1}-1)(2^m-1)}{(2^{m-1}-1)(2^{m-2}-1)\cdots(2-1)} \\ &= \frac{(2^{2m}-1)(2^{2m-1}-1)}{(2^m-1)^2} \cdot n(2m-2, m-1, 2) \\ &\geq \frac{(2^{2m}-1)(2^{2m-1}-1)}{(2^m-1)^2} \cdot 2^{(m-1)^2+\frac{1}{2}}, \quad \text{by induction.} \end{aligned}$$

We now bound $(2^{2m}-1)(2^{2m-1}-1)$. Let $f(x) = x^2 - x - 1$. Then $f(x)$ is a positive quadratic with

$$f(-1) = 1 \qquad f(0) = -1 \qquad f(2) = 1,$$

and so $f(x) > 0$ for $x \geq 2$. Therefore $\frac{1}{2}x^2 - x - 1 > -\frac{1}{2}x^2$ for $x \geq 2$, and so substituting

$x = 2^m$ obtains $2^{2m-1} - 2^m - 1 > -2^{2m-1}$. Thus

$$(2^m + 1)(2^{2m-1} - 1) = 2^{3m-1} + 2^{2m-1} - 2^m - 1 > 2^{3m-1} - 2^{2m-1} = 2^{2m-1}(2^m - 1),$$

and so

$$\begin{aligned}\frac{(2^{2m}-1)(2^{2m-1}-1)}{(2^m-1)^2}2^{(m-1)^2} &= \frac{(2^m-1)(2^m+1)(2^{2m-1}-1)}{(2^m-1)^2}2^{(m-1)^2}\\ &= \frac{(2^m+1)(2^{2m-1}-1)}{(2^m-1)}2^{(m-1)^2}\\ &> \frac{2^{2m-1}(2^m-1)}{(2^m-1)}2^{(m-1)^2}\\ &= 2^{2m-1}\cdot 2^{(m-1)^2}\\ &= 2^{m^2}.\end{aligned}$$

Therefore it follows that

$$n(2m, m, 2) > \frac{(2^{2m}-1)(2^{2m-1}-1)}{(2^m-1)^2}2^{(m-1)^2+\frac{1}{2}} > 2^{m^2+\frac{1}{2}}. \quad \square$$

Proof of Proposition 3.1.3. Let $G = \mathrm{P\Gamma L}_d(q)$ act on Ω. Then $G = \mathrm{PGL}_d(q) \rtimes C_f$ by (2.4). Hence Lemma 2.3.5 and Theorem 3.1.2 imply that

$$\mathrm{I}(G) = \mathrm{I}(\mathrm{PGL}_d(q)) + \ell(C_f) \leq (m+1)d - 2m + 1 + \log f. \tag{3.8}$$

First let $m = 1$, so that $\mathrm{I}(G) \leq 2(d-1) + 1 + \log f$ by (3.8) and $(d-1)\log q < \log n$ by Lemma 3.1.18. If $q = 2$, then $\log q = 1$ and $\log f = 0$, and so

$$\mathrm{I}(G) \leq 2(d-1) + 1 + \log f = 2(d-1)\log q + 1 < 2\log n + 1.$$

If $q > 2$, then $\frac{3}{2} < \log q$, and so

$$\mathrm{I}(G) \leq 2(d-1) + 1 + \log f < \frac{4}{3}(d-1)\log q + 1 + \log f < \frac{4}{3}\log n + 1 + \log f.$$

Now let $m = \frac{d}{2} \geq 2$, so that $\mathrm{I}(G) \leq \frac{d^2}{2} + 1 + \log f$ by (3.8). If $q = 2$, then $\frac{d^2}{4} + \frac{1}{2} < \log n$ by Lemma 3.1.18, and so

$$\mathrm{I}(G) \leq \frac{d^2}{2} + 1 < 2\log n.$$

Let $q > 2$. Then $\frac{3}{2} < \log q$ and $1 \leq \frac{d^2}{4}$, and so

$$\frac{d^2}{2} + 1 \leq \frac{3d^2}{4} < \frac{d^2}{2}\log q = 2m(d-m)\log q.$$

Combining the above with Lemma 3.1.18 gives

$$\mathrm{I}(G) \leq 2m(d-m)\log q + \log f < 2\log n + \log f.$$

Finally let $1 < m < \frac{d}{2}$. Then $2 \leq m$ and $1 \leq d - 2m$, and so

$$d - 2m + 1 \leq 2(d-2m) \leq m(d-2m).$$

Hence by (3.8)

$$\mathrm{I}(G) - \log f \leq md + d - 2m + 1 \leq md + m(d-2m) = 2m(d-m) \leq 2m(d-m)\log q.$$

Therefore, $\mathrm{I}(G) \leq 2m(d-m)\log q + \log f \leq 2\log n + \log f$ by Lemma 3.1.18. □

3.2 Lower bounds on $\mathrm{B}(\mathrm{PGL}_d(q))$ as a function of m and d

We now temporarily turn our attention from maximal irredundant bases to minimal bases of maximal size. Let q be a prime power, let $\mathbb{F} = \mathrm{GF}(q)$, let $1 \leq m \leq d$, let $V = \mathbb{F}^d$ and let $\Omega = \mathcal{PG}_m(V)$. In this section we prove the following result.

Theorem 3.2.1. *Let* $\mathrm{PGL}_d(q)$ *act on* Ω. *Then*

$$\mathrm{B}(\mathrm{PGL}_d(q)) \geq \begin{cases} (d-m)m & \text{if } q = 2, \\ (d-m)(m+1) & \text{otherwise.} \end{cases}$$

Let $G = \mathrm{GL}_d(q)$, let $l = (d-m)m$ if $q = 2$ and let $l = (d-m)(m+1)$ if $q > 2$. We construct $\Lambda = (\omega_1, \ldots, \omega_l) \in \Omega^l$, and then show that $G_\Lambda = \mathbb{F}^*I$ and that for $1 \leq i \leq l$ there exists $T_i \in G_{\Lambda\setminus\{\omega_i\}} \setminus \mathbb{F}^*I$. Hence it will follow that Λ is a minimal base for $\mathrm{PGL}_d(q)$ by Lemma 3.1.8(i), and so Theorem 3.2.1 holds. Although we redefine Λ here, in each case Λ is a subsequence of the irredundant base constructed in the proof of the lower bound of Theorem 3.1.2.

As in the previous section, for $1 \leq x, y \leq d$ and $W \subseteq V$ let $T(x,y)$ be the matrix $I + E_{x,y}$ and let $\mathrm{Supp}_x(W)$ be the set of vectors in W which are non-zero in position x. We begin with the case of $q = 2$.

Lemma 3.2.2. *Let* $\mathrm{PGL}_d(2)$ *act on* Ω. *Then*

$$\mathrm{B}(\mathrm{PGL}_d(2)) \geq (d-m)m.$$

Proof. Let $G = \mathrm{GL}_d(2)$. Since $q = 2$ it follows that $\mathbb{F}^*I = I$.

First let $(m,d) = (1,2)$ and let $\Lambda = (\langle e_1 \rangle, \langle e_2 \rangle)$. Then $G_\Lambda = I$, $T(1,2) \in G_{\Lambda\setminus\langle e_1 \rangle}$ and

$T(2,1) \in G_{\Lambda\backslash\langle e_2\rangle}$. Hence Λ is a minimal base of length $2 = (d-m)m+1$.

Therefore if $m = 1$, then we may assume that $d \geq 3 = m+2$. If $m \geq 2$, then it follows immediately that $d \geq 2m \geq m+2$. Hence for the remainder of the proof we assume that $d \geq m+2$.

Let $1 \leq s \leq d-m$ and $1 \leq r \leq m$, let

$$W_{(s-1)m+r} = \big\{e_{m+s}, e_i \;\big|\; i \in \{1,2,\dots,m\}\backslash\{r\}\big\},$$

let $\omega_{(s-1)m+r} = \langle W_{(s-1)m+r}\rangle \in \Omega$, and let $\Lambda = (\omega_1, \dots, \omega_{(d-m)m})$.

Since $d \geq m+2$ there exist $1 \leq s, s' \leq d-m$ with $s \neq s'$. Hence elements of G_Λ fix the following.

$$\left(\bigcap_{\substack{j=1\\ j\neq r}}^{m} \omega_{(s-1)m+j}\right) \cap \left(\bigcap_{\substack{j=1\\ j\neq r}}^{m} \omega_{(s'-1)m+j}\right) = \langle e_{m+s}, e_r\rangle \cap \langle e_{m+s'}, e_r\rangle = \langle e_r\rangle$$

$$\bigcap_{r=1}^{m} \omega_{(s-1)m+r} = \langle e_{m+s}\rangle$$

Therefore G_Λ fixes $\langle e_r\rangle$ for $1 \leq r \leq m$ and fixes $\langle e_{m+s}\rangle$ for $1 \leq s \leq d-m$, and so $G_\Lambda = I$.

Let $T := T(m+s, r)$ and let $\omega_{(s'-1)m+r'} \in \Lambda\backslash\{\omega_{(s-1)m+r}\}$. If $s \neq s'$, then $\mathrm{Supp}_{m+s}(W_{(s'-1)m+r'}) = \emptyset$. If $s = s'$, then $r \neq r'$ and so

$$\mathrm{Supp}_{m+s}(W_{(s-1)m+r'})T = \{e_{m+s}\}T = \{e_{m+s}+e_r\} \subseteq \omega_{(s-1)m+r'}.$$

Therefore $T \in G_{\Lambda\backslash\{\omega_{(s-1)m+r}\}}\backslash I$, and so the result follows. □

For $q > 2$ we begin by considering a few small cases. In each case we choose Λ to be consistent with the general case. Recall that for $\Lambda = (\omega_1, \dots, \omega_l) \in \Omega^l$ and for $1 \leq i \leq l$, we let $G^{(i)} = G_{\lambda_1,\dots,\lambda_i}$ and let $g^{(i)}$ be a representative element of $G^{(i)}$.

Lemma 3.2.3. *Let $(m,d) \in \big\{(1,2),(1,3),(2,4)\big\}$, let $q > 2$ and let $G = \mathrm{PGL}_d(q)$ act on Ω. Then*

$$\mathrm{B}(\mathrm{PGL}_d(q)) \geq (d-m)(m+1).$$

Proof. Let $G = \mathrm{GL}_d(q)$. First let $(m,d) = (1,2)$ and let

$$\Lambda = (\omega_1, \omega_2, \omega_3) = (\langle e_1\rangle, \langle e_2\rangle, \langle e_1+e_2\rangle).$$

Then Λ has length $3 > 2 = (d-m)(m+1)$. Now

$$g^{(1)} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}, \quad g^{(2)} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \quad \text{and} \quad g^{(3)} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

and so $G_\Lambda = \mathbb{F}^* I$. In addition

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \in G_{\Lambda \backslash \{\omega_1\}}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \in G_{\Lambda \backslash \{\omega_2\}}, \qquad \text{and} \qquad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in G_{\Lambda \backslash \{\omega_3\}}.$$

Now let $(m, d) = (1, 3)$ and let

$$\Lambda = (\omega_1, \omega_2, \omega_3, \omega_4) = (\langle e_2 \rangle, \langle e_3 \rangle, \langle e_1 + e_2 \rangle, \langle e_1 + e_3 \rangle).$$

Then Λ has length $4 = (d-m)(m+1)$. In addition

$$g^{(1)} = \begin{pmatrix} * & * & * \\ 0 & * & 0 \\ * & * & * \end{pmatrix} \; g^{(2)} = \begin{pmatrix} * & * & * \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \; g^{(3)} = \begin{pmatrix} \lambda & \mu & 0 \\ 0 & \lambda - \mu & 0 \\ 0 & 0 & * \end{pmatrix} \; g^{(4)} = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix},$$

and so $G_\Lambda = \mathbb{F}^* I$.

Let $T_1 = I + E_{2,1} + E_{2,2}$. Then T_1 fixes ω_2 and ω_4 pointwise, and sends $v \in \omega_3$ to $2v$, thus $T_1 \in G_{\lambda \backslash \{\omega_1\}} \backslash \mathbb{F}^* I$. Similarly $T_2 = I + E_{3,1} + E_{3,3}$ fixes ω_1 and ω_3 pointwise, and sends $v \in \omega_4$ to $2v$, hence $T_2 \in G_{\lambda \backslash \{\omega_2\}} \backslash \mathbb{F}^* I$. Now $T_3 = T(2, 2)$ fixes ω_2 and ω_4 pointwise, and sends $v \in \omega_1$ to $2v$, and so $T_3 \in G_{\lambda \backslash \{\omega_3\}} \backslash \mathbb{F}^* I$. Finally $T_4 = I + E_{1,1} + E_{1,2}$ fixes ω_1 and ω_2 pointwise, and sends $v \in \omega_3$ to $2v$, and so $T_4 \in G_{\lambda \backslash \{\omega_4\}} \backslash \mathbb{F}^* I$.

Finally let $(m, d) = (2, 4)$, let

$$(W_1, \ldots, W_6) = (\{e_1, e_4\}, \{e_2, e_4\}, \{e_1 + e_2, e_3\}, \{e_1 + e_3, e_2\}, \{e_1 + e_4, e_2\}, \{e_2, e_3\}),$$

and for $1 \leq k \leq 6$ let $\omega_k = \langle W_k \rangle$ and $g^{(k)} \in G^{(k)}$. Then $\Lambda = (\omega_1, \ldots, \omega_6) \in \Omega^6$ has length $(d-m)(m+1)$ and the following hold.

$$g^{(1)} = \begin{pmatrix} * & 0 & 0 & * \\ * & * & * & * \\ * & * & * & * \\ * & 0 & 0 & * \end{pmatrix} \qquad g^{(2)} = \begin{pmatrix} * & 0 & 0 & * \\ 0 & * & 0 & * \\ * & * & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \qquad g^{(3)} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ \mu & \mu & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix}$$

$$g^{(4)} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ \mu & \mu & \lambda+\mu & 0 \\ 0 & 0 & 0 & * \end{pmatrix} \quad g^{(5)} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ \mu & \mu & \lambda+\mu & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix} \quad g^{(6)} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Therefore $G_\Lambda = \mathbb{F}^* I$.

Let $T_1 = T(4,2)$. Then $\text{Supp}_4(W_3) = \text{Supp}_4(W_4) = \text{Supp}_4(W_6) = \emptyset$,

$$\text{Supp}_4(W_2)T_1 = \{e_4\}T_1 = \{e_2 + e_4\} \subseteq \omega_2, \text{ and}$$

$$\text{Supp}_4(W_5)T_1 = \{e_1 + e_4\}T_1 = \{e_1 + e_2 + e_4\} \subseteq \omega_5.$$

Hence $T_1 \in G_{\Lambda\backslash\{\omega_1\}}\backslash\mathbb{F}^* I$. Now let $T_2 = 2I - E_{4,1} - E_{4,4}$. Then T_2 sends vectors $v \in \omega_3 \cup \omega_4 \cup \omega_6$ to $2v$,

$$\omega_1 T_2 = \langle e_1, e_4\rangle T_2 = \langle 2e_1, -e_1 + e_4\rangle = \omega_1 \text{ and}$$

$$\omega_5 T_2 = \langle e_1 + e_4, e_2\rangle T_2 = \langle e_1 + e_4, 2e_2\rangle = \omega_5.$$

Hence $T_2 \in G_{\Lambda\backslash\{\omega_2\}}\backslash\mathbb{F}^* I$. Let $T_3 = T(2,2)$. Then $\text{Supp}_2(\omega_1) = \emptyset$, and if $k \neq 1, 3$ then

$$\text{Supp}_2(W_k)T_3 = \{e_2\}T_3 = \{2e_2\} \subseteq \omega_k.$$

Hence $T_3 \in G_{\Lambda\backslash\{\omega_3\}}\backslash\mathbb{F}^* I$. Let $T_4 = T(3,3)$. Then $\text{Supp}_3(\omega_1), \text{Supp}_3(\omega_2)$ and $\text{Supp}_3(\omega_5)$ are empty, and if $k \in \{3, 6\}$ then

$$\text{Supp}_3(W_k)T_4 = \{e_3\}T_4 = \{2e_3\} \subseteq \omega_k.$$

Hence $T_4 \in G_{\Lambda\backslash\{\omega_4\}}\backslash\mathbb{F}^* I$. Let $T_5 = T(4,4)$. Then $\text{Supp}_4(\omega_3), \text{Supp}_4(\omega_4)$ and $\text{Supp}_4(\omega_6)$ are empty, and for $k \in \{1, 2\}$ then

$$\text{Supp}_4(W_k)T_5 = \{e_4\}T_5 = \{2e_4\} \subseteq \omega_k.$$

Hence $T_5 \in G_{\Lambda\backslash\{\omega_5\}}\backslash\mathbb{F}^* I$. Finally, let $T_6 = 2I - E_{3,1} - E_{3,2} - E_{3,3}$. Then T_2 sends vectors $v \in \omega_1 \cup \omega_2 \cup \omega_5$ to $2v$,

$$\omega_3 T_6 = \langle e_1 + e_2, e_3\rangle T_6 = \langle 2e_1 + 2e_2, -e_1 - e_2 + e_3\rangle = \omega_3 \text{ and}$$

$$\omega_4 T_6 = \langle e_1 + e_3, e_2\rangle T_6 = \langle e_1 - e_2 + e_3, 2e_2\rangle = \omega_4.$$

Hence $T_6 \in G_{\Lambda\backslash\{\omega_6\}}\backslash\mathbb{F}^*I$, and the result follows. □

We now complete Theorem 3.2.1.

Proof of Theorem 3.2.1. If $q = 2$ then the result holds by Lemma 3.2.2, and so assume that $q > 2$. If $(m, d) \in \big\{(1,2),(1,3),(2,4)\big\}$, then the result holds by Lemma 3.2.3. Hence if $m = 1$, then $d \geq 4 = m+3$; if $m = 2$, then $d \geq 5 = m+3$; and if $m \geq 3$, then it follows immediately that $d \geq 2m \geq m+3$. Hence in all cases $d \geq m+3$.

Let $G = \mathrm{GL}_d(q)$. Consider the following sets of m linearly independent vectors.

$$\begin{aligned}
W_{(s-2)m+r} &= \big\{e_{m+s}, e_i \;\big|\; i \in \{1,2,\ldots,m\}\backslash\{r\}\big\} && 2 \leq s \leq d-m,\;\; 1 \leq r \leq m\\
W_{(d-m-1)m+t} &= \big\{e_1 + e_{t+1}, e_i \;\big|\; i \in \{2,\ldots,m,m+1\}\backslash\{t+1\}\big\} && 1 \leq t \leq m\\
W_{(d-m)m+u} &= \big\{e_1 + e_{m+1+u}, e_i \;\big|\; i \in \{2,\ldots,m\}\big\} && 1 \leq u \leq d-m-1\\
W_{(d-m)(m+1)} &= \big\{e_2,\ldots,e_{m+1}\big\}
\end{aligned}$$

Let $1 \leq k \leq (d-m)(m+1)$, let $\omega_k = \langle W_k\rangle$ and let $\Lambda = (\omega_1,\ldots,\omega_{(d-m)(m+1)})$ be in $\Omega^{(d-m)(m+1)}$.

We show in three stages that $G_\Lambda = \mathbb{F}^*I$. We begin by showing that G_Λ fixes $\langle e_i\rangle$ for $1 \leq i \leq d$. Since $d \geq m+3$, there exists $2 \leq s, s' \leq d-m$ with $s \neq s'$. Let $1 \leq r \leq m$, $1 \leq t \leq m$, and $1 \leq u \leq d-m-1$. Elements of G_Λ fix the following.

$$\left(\bigcap_{\substack{j=1\\j\neq r}}^{m} \omega_{(s-2)m+j}\right) \cap \left(\bigcap_{\substack{j=1\\j\neq r}}^{m} \omega_{(s'-2)m+j}\right) = \langle e_{m+s}, e_r\rangle \cap \langle e_{m+s'}, e_r\rangle = \langle e_r\rangle$$

$$\begin{aligned}
\left(\bigcap_{t=1}^{m-1} \omega_{(d-m-1)m+t}\right) \cap \omega_{(d-m)(m+1)} &= \langle e_1 + e_2 + \cdots + e_m, e_{m+1}\rangle \cap \langle e_2,\ldots,e_m,e_{m+1}\rangle\\
&= \langle e_{m+1}\rangle
\end{aligned}$$

$$\bigcap_{r=1}^{m} \omega_{(s-2)m+r} = \langle e_{m+s}\rangle$$

Therefore G_Λ fixes $\langle e_r\rangle$ for $1 \leq r \leq m$, fixes $\langle e_{m+1}\rangle$, and fixes $\langle e_{m+s}\rangle$ for $2 \leq s \leq d-m$. Thus G_Λ fixes $\langle e_i\rangle$ for $1 \leq i \leq d$. Hence if $g \in G_\Lambda$ then $g_{ij} = 0$ for $i \neq j$.

We now show that G_Λ fixes $\langle e_1 + e_i\rangle$ for $i \neq m+1$. Let $2 \leq s \leq d-m$ and $2 \leq r \leq m$.

Then G_Λ fixes the following.

$$\begin{aligned}\left(\bigcap_{\substack{j=2\\ j\neq r}}^{m}\omega_{(s-2)m+j}\right)\cap\omega_{(d-m-1)m+(r-1)} &= \langle e_{m+s}, e_1, e_r\rangle \cap \big\langle e_1+e_r, e_i \bigm| i\in\{2,\dots,m+1\}\backslash\{r\}\big\rangle\\ &= \langle e_1+e_r\rangle\\ \left(\bigcap_{r=2}^{m}\omega_{(s-2)m+r}\right)\cap\omega_{(d-m)m+(s-1)} &= \langle e_1, e_{m+s}\rangle \cap \big\langle e_1+e_{m+s}, e_i \bigm| i\in\{2,\dots,m\}\big\rangle\\ &= \langle e_1+e_{m+s}\rangle\end{aligned}$$

Therefore G_Λ fixes $\langle e_1+e_r\rangle$ for $2\le r\le m$, and $\langle e_1+e_{m+s}\rangle$ for $2\le s\le m-d$. Thus G_Λ fixes $\langle e_1+e_i\rangle$ for $i\neq m+1$. Let $g\in G_\Lambda$. We have previously shown that $g_{ij}=0$ for $i\neq j$, and now it follows that $g_{ii}=g_{11}$ for $i\neq m+1$.

Finally G_Λ fixes

$$\bigcap_{t=1}^{m}\omega_{(d-m-1)m+t} = \langle e_1+e_2+\cdots+e_{m+1}\rangle.$$

Let $g\in G_\Lambda$. Then $g_{ij}=0$ for $i\neq j$, and $g_{ii}=g_{11}$ for $i\neq m+1$ by the previous argument, and now it follows that $g_{11}=g_{22}=\cdots=g_{m+1,m+1}$. Hence $g=g_{11}I$, and so $G_\Lambda=\mathbb{F}^*I$.

It remains to find $T_i\in G_{\Lambda\backslash\{\omega_i\}}\backslash F^*I$ for $1\le i\le (d-m)(m+1)$. First let $r=1$, let $2\le s\le d-m$ and let

$$T=T_{(s-2)m+1}=2I-E_{m+s,m+s}-E_{m+s,1}.$$

Let $k\neq (s-2)m+1$ and let $v\in\omega_k$. If $\mathrm{Supp}_{m+s}(\{v\})=\emptyset$, then $vT=2v$. Therefore if $\mathrm{Supp}_{m+s}(W_k)T\subseteq\omega_k$, then it follows that $\omega_kT=\omega_k$. Thus for $2\le r'\le m$

$$\mathrm{Supp}_{m+s}(W_k)T=\begin{cases}\{e_{m+s}\}T=\{-e_1+e_{m+s}\}\subseteq\omega_k & \text{if } k=(s-2)m+r',\\ \{e_1+e_{m+s}\}T=\{e_1+e_{m+s}\}\subseteq\omega_k & \text{if } k=(d-m)m+(s-1),\\ \emptyset & \text{otherwise,}\end{cases}$$

and so $T\in G_{\Lambda\backslash\{\omega_{(s-2)m+1}\}}\backslash\mathbb{F}^*I$. Now let $r\ge 2$, let $2\le s\le d-m$ and let

$$T=T_{(s-2)m+r}=T(m+s,r).$$

Let $1\le r'\le m$ with $r'\neq r$ and let $k\neq (s-2)m+r$ then

$$\mathrm{Supp}_{m+s}(W_k)T=\begin{cases}\{e_{m+s}\}T=\{e_r+e_{m+s}\}\subseteq\omega_k & \text{if } k=(s-2)m+r',\\ \{e_1+e_{m+s}\}T=\{e_1+e_{m+s}+e_r\}\subseteq\omega_k & \text{if } k=(d-m)m+(s-1),\\ \emptyset & \text{otherwise.}\end{cases}$$

Hence $T \in G_{\Lambda \setminus \{\omega_{(s-2)m+r}\}} \setminus \mathbb{F}^* I$.

Let $1 \leq t \leq m$ and let $T = T_{(d-m-1)m+t} = T(t+1, t+1)$. If $t = m$, then let $k \neq (d-m-1)m + m$ and let $1 \leq t' \leq m-1$. Then

$$\mathrm{Supp}_{m+1}(W_k) = \begin{cases} \{e_{m+1}\}T = \{2e_{m+1}\} \subseteq \omega_k & \text{if } k = (d-m-1)m + t' \text{ or } (d-m)(m+1), \\ \emptyset & \text{otherwise.} \end{cases}$$

Hence $T \in G_{\Lambda \setminus \{\omega_{(d-m-1)m+m}\}} \setminus \mathbb{F}^* I$. Now let $t \leq m-1$, let $k \neq (d-m-1)m+t$ and let $2 \leq s \leq d-m$. Then

$$\mathrm{Supp}_{t+1}(W_k) = \begin{cases} \emptyset & \text{if } k = (s-2)m + (t+1), \\ \{e_{t+1}\}T = \{2e_{t+1}\} \subseteq \omega_k & \text{otherwise.} \end{cases}$$

Hence $T \in G_{\Lambda \setminus \{\omega_{(d-m-1)m+t}\}} \setminus \mathbb{F}^* I$.

Let $1 \leq u \leq d-m-1$, let $T = T_{(d-m)m+u} = T(m+1+u, m+1+u)$, let $k \neq (d-m)m+u$ and let $1 \leq r \leq m$. Then

$$\mathrm{Supp}_{m+1+u}(W_k)T = \begin{cases} \{e_{m+1+u}\}T = \{2e_{m+1+u}\} \subseteq \omega_k & \text{if } k = (u-1)m + r, \\ \emptyset & \text{otherwise.} \end{cases}$$

Hence $T \in G_{\Lambda \setminus \{\omega_{(d-m)m+u}\}} \setminus \mathbb{F}^* I$.

Finally, let $T = T_{(d-m)(m+1)} = I + \sum_{i=1}^{m+1} E_{m+1,i}$, so that

$$e_i T = \begin{cases} \sum_{i=1}^{m} e_i + 2e_{m+1} & \text{if } i = m+1, \\ e_i & \text{otherwise.} \end{cases}$$

Hence by the above, $\omega_k T = \omega_k$ if and only if $\mathrm{Supp}_{m+1}(W_k)T \subseteq \omega_k$. Let $k \neq (d-m)(m+1)$ and let $1 \leq t \leq m-1$. Then

$$\mathrm{Supp}_{m+1}(W_k)T$$
$$= \begin{cases} \{e_{m+1}\}T = \{\sum_{i=1}^{m} e_i + 2e_{m+1}\} \subseteq \omega_{(d-m-1)m+t} & \text{if } k = (d-m-1)m+t, \\ \{e_1 + e_{m+1}\}T = \{2(e_1 + e_{m+1}) + \sum_{i=2}^{m} e_i\} \subseteq \omega_{(d-m-1)m+t} & \text{if } k = (d-m-1)m+m, \\ \emptyset & \text{otherwise.} \end{cases}$$

Hence $T \in G_{\Lambda \setminus \{\omega_{(d-m)(m+1)}\}} \setminus \mathbb{F}^* I$. □

3.3 Almost simple groups

In this section we prove Theorem 3.0.3 for almost simple groups. More precisely we prove the following result.

Theorem 3.3.1. *Let G be an almost simple primitive subgroup of* $\mathrm{Sym}(\Omega)$*. If G is not large base, then*

$$\mathrm{I}(G,\Omega) < 5\log|\Omega| - 1.$$

By Lemma 2.7.14 the proof of Theorem 3.3.1 can be divided into proving the result for the following possibilities of G, G_0 and Ω:

(I) $\mathrm{b}(G,\Omega) \leq 6$ or $G = \mathrm{M}_{24}$ in its natural action on $\{1,\dots,24\}$;

(II) $G_0 = \mathrm{Alt}(l)$ and Ω is an orbit of subsets or partitions of $\{1,\dots,l\}$;

(III) $G_0 = \mathrm{PSL}_d(q)$ and $\Omega = \mathcal{PG}_m(V)$ with $m \leq \frac{n}{2}$;

(IV) $G_0 = \mathrm{PSL}_d(q)$ and $\Omega = \Omega_m^{\oplus}$;

(V) $G_0 = \mathrm{PSL}_d(q)$ and $\Omega = \Omega_m^{<}$;

(VI) $G_0 = \mathrm{PSp}_d(2^f)$ and Ω is the set of cosets of $\mathrm{N}_G(O_d^{\pm}(2^f))$ in G;

(VII) $G_0 = \mathrm{P}\Omega_8^+(q)$;

(VIII) $G_0 = \mathrm{P}\Omega_d^+(q)$ with $d \geq 10$ and $\Omega \subseteq \mathcal{PG}_{\frac{d}{2}}(V)$; or

(IX) $G \leq \mathrm{P\Gamma L}_d(q)$ with $d \geq 3$ and $\Omega \subseteq \mathcal{PG}_m(V)$ such that $m \leq \frac{d}{2}$ and $|\Omega| > q^{\frac{1}{2}m(d-m)}$.

This section is split into three subsections. In the first we consider Case (I), and in the second we consider Case (III), (IV) and (V). In the third we consider Cases (VII), (VIII) and (IX), and then by quoting results from [28] for Cases (II) and (VI) we complete the proof of Theorem 3.3.1.

3.3.1 Case (I)

In this subsection we prove the lemma below. From which Theorem 3.3.1 holds for Case (I) since $n \geq 5$ by Lemma 2.6.5, and so $1 \leq \log n - 1$.

Lemma 3.3.2. *Let $G \leq \mathrm{Sym}(\Omega)$ be as in Case* (I) *and let $n = |\Omega|$. Then*

$$\mathrm{I}(G,\Omega) \leq 4\log n + 1.$$

Throughout, let Ω be a finite set of size n, and let G be a primitive subgroup of $\mathrm{Sym}(\Omega)$. We begin with a some preliminary cases and lemmas. We denote the minimal index of a proper subgroup of G by $m(G)$. Hence for $H \lneq G$, it follows that $m(G) \leq [G : H]$.

Lemma 3.3.3. *Let G be a transitive subgroup of S_n with point stabilizer H. If H is insoluble and either $|G| \leq m(G)^5$ or $|H| \leq [G:H]^4$, then*

$$\mathrm{I}(G) \leq 4 \log n.$$

Proof. We first show that $|G| \leq m(G)^5$ implies that $|H| \leq [G:H]^4$. Since $m(G) \leq [G:H]$, it follows that

$$|H| = \frac{|G|}{[G:H]} \leq \frac{m(G)^5}{[G:H]} \leq [G:H]^4.$$

Hence we may assume that $|H| \leq [G:H]^4$.

Since H is insoluble it follows that $\mathrm{I}(H) + 1 \leq \log |H|$ by Lemma 2.3.1(i). Since G is transitive and H is a point stabilizer, we deduce that $\mathrm{I}(G) = \mathrm{I}(H) + 1$ and $[G:H] = n$. Therefore

$$\mathrm{I}(G) = \mathrm{I}(H) + 1 \leq \log |H| \leq \log[G:H]^4 = 4 \log n. \quad \square$$

Lemma 3.3.4. *Let G be a subgroup of $\mathrm{Sym}(\Omega)$ with socle G_0 and point stabilizer H, let $n = |\Omega|$ and let $q = p^f$ be a prime power. If*

$$(G_0, H) \in \Big\{ \big(E_6(q), P_1\big), \big(E_6(q), P_6\big), \big(E_7(q), P_7\big) \Big\},$$

then $I(G) < 4 \log n$.

Proof. In each case H is insoluble by Lemma 2.1.8. We now show that $|G| < m(G)^5$, and so the result will follow by Lemma 3.3.3.

First let $G_0 = E_6(q)$. By [20, Table 5 and 6]

$$|E_6(q)| = \frac{q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)}{(3, q-1)}$$

and $|\mathrm{Out}(E_6(q))| \leq 2f(3, q-1) < q(3, q-1)$. Hence

$$|G| \leq q^{37}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1) < q^{37+12+9+8+6+5+2} = q^{79}.$$

By [57, p2]

$$m(G) \geq m(G_0) \geq \frac{(q^9-1)(q^8+q^4+1)}{q-1} = (q^8+q^7+\cdots+q+1)(q^8+q^4+1) > q^{8+8} = q^{16}.$$

Hence $|G| < q^{79} < q^{80} < m(G)^5$.

Now let $G_0 = E_7(q)$. By [20, Table 5 and 6]

$$|E_7(q)| = \frac{q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)}{(2,q-1)}$$

and $|\mathrm{Out}(E_7(q))| = f(2,q-1) < q(2,q-1)$. Hence

$$|G| \leq q^{64}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1) < q^{64+18+14+12+10+8+6+2} = q^{134}.$$

By [57, p5]

$$m(G) = \frac{(q^{14}-1)(q^9+1)(q^5+1)}{q-1} = (q^{13}+q^{12}+\cdots+q+1)(q^9+1)(q^5+1) > q^{13+9+5} = q^{27}.$$

Hence $|G| < q^{134} < q^{135} < m(G)^5$. □

We can now prove Lemma 3.3.2.

Proof of Lemma 3.3.2. Let $G \leq \mathrm{Sym}(\Omega)$ be as in Case (I), so that either $\mathrm{b}(G,\Omega) \leq 6$ or $(G,\Omega) = (\mathrm{M}_{24}, \{1,\ldots,24\})$. If $\mathrm{b}(G,\Omega) \leq 5$, then the result holds by Lemma 2.3.1(iii), and by [28, p10]

$$\mathrm{I}(\mathrm{M}_{24}, \{1,\ldots,24\}) = 7 < 2\log 24.$$

Hence we may assume that $\mathrm{b}(G,\Omega) = 6$.

Let G have point stabilizer H. By a result of Burness [6] it follows that either

$$(G,H) \in \Big\{ \big(\mathrm{M}_{23}, \mathrm{M}_{22}\big), \big(\mathrm{Co}_3, \mathrm{McL}.2\big), \big(\mathrm{Co}_2, \mathrm{U}_6(2).2\big), \big(\mathrm{Fi}_{22}.2, 2.\mathrm{U}_6(2).2\big) \Big\} \text{ or} \tag{3.9}$$

$$\big(\mathrm{soc}(G), H\big) \in \Big\{ \big(E_6(q), P_1\big), \big(E_6(q), P_6\big), \big(E_7(q), P_7\big) \Big\}. \tag{3.10}$$

If G is as in (3.10), then the result holds by Lemma 3.3.4. Hence assume that G satisfies (3.9).

First let $(G,H) = (\mathrm{M}_{23}, \mathrm{M}_{22})$. Then G is the point stabilizer of M_{24} in its action on 24 points, and so

$$\mathrm{I}(G) = \mathrm{I}(\mathrm{M}_{24}) - 1 = 6 < 2\log 23.$$

For the remaining cases we proceed using [20, p100,115,134,156]. Since McL and $\mathrm{U}_6(2)$ are non-abelian simple, it follows that H is insoluble by Lemma 2.1.7. We now show that $|H| < [G:H]^4$, and so the result will follow by Lemma 3.3.3. If $(G,H) = (\mathrm{Co}_3, \mathrm{McL}.2)$, then

$$|H| = 2^8 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 < 276^4 = [G:H]^4.$$

If $(G,H) = (\mathrm{Co}_2, \mathrm{U}_6(2).2)$, then

$$|H| = 2^{16} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11 < 2300^4 = [G:H]^4.$$

Finally, if $(G, H) = (\mathrm{Fi}_{22}.2, 2.\mathrm{U}_6(2).2)$, then

$$|H| = 2^{16} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11 < 3510^4 = [G : H]^4.$$

Hence the result follows. $\square$

3.3.2 Cases (III), (IV) and (V)

Let $q = p^f$ be a prime power, let $\mathbb{F} = \mathrm{GF}(q)$, let $1 \leq m \leq \frac{d}{2}$, let $V = \mathbb{F}^d$, let G be almost simple with socle $\mathrm{PSL}_d(q)$ in a subspace action on $\Omega = \mathcal{PG}_m(V)$. Hence $(d, q) \neq (2, 2), (2, 3)$ by Theorem 2.5.2. We use the results in Section 3.1 to prove that Theorem 3.3.1 holds for Cases (III), (IV) and (V).

We begin with a preliminary lemma.

Lemma 3.3.5. *Let q, p, f, m and d be as above. Then*

$$m(d-m)\log q \geq \begin{cases} \log f + 1 & \text{if } m = 1, \\ 3\log f + 4 & \text{if } m \geq 2. \end{cases}$$

Proof. We first claim that $f \geq \log f + 1$. Let $y := y(f) = f - \log f - 1$. Then $\frac{dy}{df} = 1 - \frac{1}{f \ln 2}$, and so $\frac{dy}{df} = 0$ if and only if $f = \frac{1}{\ln 2} < 2$. Since $\frac{dy}{df}(2) > 0$ and $y(2) = y(1) = 0$ it follows that $y \geq 0$ for $f \in \mathbb{N}$. Therefore the claim follows.

If $m = 1$, then

$$m(d-m)\log q = (d-1)\log q = (d-1)f\log p \geq f \geq \log f + 1.$$

Now let $m \geq 2$. Then $m(d-m) \geq m(2m-m) = m^2 \geq 4$, and so

$$m(d-m)\log q \geq 4\log q \geq 3\log q + 1 = 3f\log p + 1 \geq 3f + 1 \geq 3(\log f + 1) + 1 = 3\log f + 4 \quad \square$$

The following proves Theorem 3.3.1 for Case (III).

Proposition 3.3.6. *Let G be almost simple with socle $\mathrm{PSL}_d(q)$ acting on $\Omega = \mathcal{PG}_m(V)$, and let $n = |\Omega|$. Then*

$$\mathrm{I}(G) < 3\log n.$$

Proof. If $m = 1$, then $G \leq \mathrm{P\Gamma L}_d(q)$ by Lemma 2.7.5, and so $\mathrm{I}(G) \leq \mathrm{I}(\mathrm{P\Gamma L}_d(q))$ by Lemma 2.3.3. If $m > 1$ then $G \cap \mathrm{P\Gamma L}_d(q)$ has index at most two in G, so by Lemma 2.3.3 and Corollary 2.3.6

$$\mathrm{I}(G) \leq \mathrm{I}(G \cap \mathrm{P\Gamma L}_d(q)) + 1 \leq \mathrm{I}(\mathrm{P\Gamma L}_d(q)) + 1.$$

Therefore we can bound $\mathrm{I}(G)$ by $\mathrm{I}(\mathrm{P\Gamma L}_d(q))$ when $m = 1$, and by $\mathrm{I}(\mathrm{P\Gamma L}_d(q)) + 1$ when $m > 1$. Thus $\mathrm{I}(G) \leq 2 \log n + \log f + 1$ by Proposition 3.1.3. Combining Lemmas 3.1.18 and 3.3.5 gives $\log f + 1 \leq m(d - m) \log q < \log n$, hence the result follows. □

We now consider the action of G on $\Omega_m^{\oplus}$ and $\Omega_m^{<}$ as in Definition 2.7.7. Recall that $\frac{d}{2} > m \geq 1$ in both cases, and so $d \geq 3$.

Lemma 3.3.7. *Let G be a primitive almost simple group with socle $\mathrm{PSL}_d(q)$, let $H = G \cap \mathrm{P\Gamma L}_d(q)$ and let Ω be either $\Omega_m^{\oplus}$ or $\Omega_m^{<}$. Then*

$$\mathrm{I}(G, \Omega) \leq 2\mathrm{I}(H, \mathcal{PG}_m(V)) + 1.$$

Proof. We first show that $\mathrm{I}(H, \Omega) \leq \mathrm{I}(H, \mathcal{PG}_m(V)) + \mathrm{I}(H, \mathcal{PG}_{d-m}(V))$.

Let $l = \mathrm{I}(H, \Omega)$ and let $\Lambda = \big(\{U_1, W_1\}, \ldots, \{U_l, W_l\}\big)$ be a corresponding base with $\dim(U_i) = m$ for all $1 \leq i \leq l$. Then $\Pi := (U_1, \ldots, U_l) \in \mathcal{PG}_m(V)^l$ and $\Sigma := (W_1, \ldots, W_l) \in \mathcal{PG}_{d-m}(V)^l$. By Lemma 2.3.2 there exist a subsequence of Π and of Σ which can be extended to an irredundant base for the action of H on $\mathcal{PG}_m(V)$ and $\mathcal{PG}_{d-m}(V)$ respectively.

Let Π' be the subsequence of Π which contains U_1, and for $i \geq 2$ contains U_i if and only if $H_{U_1,\ldots,U_{i-1}} > H_{U_1,\ldots,U_{i-1},U_i}$. Then Π' can be extended to an irredundant base for the action of H on $\mathcal{PG}_m(V)$. Let k be the length of Π', so that $k \leq \mathrm{I}(H, \mathcal{PG}_m(V))$.

Let $\Sigma' = (W_{j_1}, \ldots, W_{j_{(l-k)}})$ be the subsequence of Σ which contains W_i if and only if $H_{U_1,\ldots,U_{i-1}} = H_{U_1,\ldots,U_{i-1},U_i}$. Assume, for a contradiction, that Σ' cannot be extended to an irredundant base for the action of H on $\mathcal{PG}_{d-m}(V)$. Since H is irreducible, $H > H_{W_{j_1}}$, and so there exists $s \geq 2$ such that

$$H_{W_{j_1},\ldots,W_{j_{(s-1)}}} = H_{W_{j_1},\ldots,W_{j_{(s-1)}},W_{j_s}}.$$

Let $i = j_s$. Then intersecting both sides of the above expression with $H_{W_1,\ldots,W_{i-1}}$ gives

$$H_{W_1,\ldots,W_{i-1}} = H_{W_1,\ldots,W_{i-1},W_i}. \tag{3.11}$$

Since $W_i \in \Sigma'$ it follows that

$$H_{U_1,\ldots,U_{i-1}} = H_{U_1,\ldots,U_{i-1},U_i}. \tag{3.12}$$

Elements of $H = G \cap \mathrm{P\Gamma L}_d(q)$ cannot map U_i to W_i. Therefore (3.11) and (3.12) imply that

$$H_{\{U_1,W_1\},\ldots,\{U_{i-1},W_{i-1}\}} = H_{\{U_1,W_1\},\ldots,\{U_{i-1},W_{i-1}\},\{U_i,W_i\}},$$

a contradiction since Λ is irredundant. Hence $l-k \leq \mathrm{I}(H, \mathcal{PG}_{n-m}(V))$, and so

$$\mathrm{I}(H,\Omega) = l = k + (l-k) \leq \mathrm{I}(H, \mathcal{PG}_m(V)) + \mathrm{I}(H, \mathcal{PG}_{d-m}(V)). \tag{3.13}$$

Now Lemma 2.7.4 implies that $\mathrm{I}(H, \mathcal{PG}_m(V)) = \mathrm{I}(H, \mathcal{PG}_{n-m}(V))$, and so $\mathrm{I}(H,\Omega) \leq 2\mathrm{I}(H, \mathcal{PG}_m(V))$ by (3.13). Since H has index at most 2 in G, the result follows by Corollary 2.3.6. □

We now prove Theorem 3.3.1 for Cases (IV) and (V).

Lemma 3.3.8. *Let Ω be either $\Omega_m^{\oplus}$ or $\Omega_m^{<}$, let $n = |\Omega|$, and let G be an almost simple subgroup of* $\mathrm{Sym}(\Omega)$ *with socle* $\mathrm{PSL}_d(q)$. *Then*

$$\mathrm{I}(G) < 5(\log n - 1).$$

Proof. Let $H = G \cap \mathrm{P\Gamma L}_d(q)$, then by Proposition 3.1.3 and Lemma 3.3.7

$$\mathrm{I}(G) \leq 2\mathrm{I}(H, \mathcal{PG}_m) + 1 \leq \begin{cases} 4(d-1)+3 & \text{if } m=1 \text{ and } q=2, \\ \frac{8}{3}(d-1)\log q + 2\log f + 3 & \text{if } m=1 \text{ and } q \geq 3, \\ 4m(d-m)\log q + 2\log f + 1 & \text{otherwise.} \end{cases} \tag{3.14}$$

By Lemma 2.7.9 $n \geq 2|\mathcal{PG}_m(V)|$, and so Lemma 3.1.18 gives

$$\log n - 1 = \log \frac{n}{2} \geq \log|\mathcal{PG}_m(V)| > \begin{cases} \frac{d^2}{4} + \frac{1}{2} & \text{if } q=2 \text{ and } m = \frac{d}{2} \geq 2, \\ m(d-m)\log q & \text{otherwise.} \end{cases} \tag{3.15}$$

First let $m=1$. If $(d,q) = (3,2)$, then by Lemma 2.7.8

$$|\Omega_m^{\oplus}| = \frac{2^2(2^3-1)}{(2-1)} = 28 \quad \text{and} \quad |\Omega_m^{<}| = \frac{(2^2-1)(2^3-1)}{(2-1)^2} = 21.$$

By (3.14) it follows that $\mathrm{I}(G) \leq 11$. Hence

$$\mathrm{I}(G) \leq 11 < 5(\log(21) - 1) \leq 5(\log n - 1),$$

and so the result holds for $(m,d,q) = (1,3,2)$. Therefore if $m=1$ and $q=2$, then we may assume that $d \geq 4$, and so

$$\begin{aligned} \mathrm{I}(G) &\leq 4(d-1)+3 && \text{by (3.14),} \\ &\leq 5(d-1) && \text{since } d-1 \geq 3, \\ &< 5(\log n - 1) && \text{by (3.15).} \end{aligned}$$

Therefore let $m = 1$ and let $q \geq 3$. Then

$$\begin{aligned}
\mathrm{I}(G) &\leq \tfrac{8}{3}(d-1)\log q + 2\log f + 3 && \text{by (3.14)},\\
&\leq \tfrac{8}{3}(d-1)\log q + 2(d-1)\log q + 1 && \text{by Lemma 3.3.5},\\
&< 5(d-1)\log q && \text{since } 1 < \tfrac{1}{3}(d-1)\log q,\\
&< 5(\log n - 1) && \text{by (3.15)}.
\end{aligned}$$

Finally, let $m \geq 2$. Then

$$\begin{aligned}
\mathrm{I}(G) &\leq 4m(d-m)\log q + 2\log f + 1 && \text{by (3.14)}\\
&\leq 5m(d-m)\log q && \text{by Lemma 3.3.5}\\
&< 5(\log n - 1) && \text{by (3.15)}. \quad \square
\end{aligned}$$

3.3.3 Proof of Theorem 3.3.1

Here we prove Theorem 3.3.1. We begin by considering Cases (VII), (VIII) and (IX). Let $q = p^f$ be a prime power, let $\mathbb{F} = \mathrm{GF}(q)$, let $1 \leq m \leq \frac{d}{2}$, let $V = \mathbb{F}^d$ and let $\Omega = \mathcal{PG}_m(V)$.

The following lemma will be used for Case (VII).

Lemma 3.3.9. *If $q \geq 3$, then $q^2 > 6f$.*

Proof. Fix q, let $f \geq 1$ and let

$$y = y(f) = q^2 - 6f = p^{2f} - 6f.$$

Then

$$\frac{dy}{df} = 2\ln(p)p^{2f} - 6 > p^{2f} - 6 = q^2 - 6 \geq 9 - 6 > 0.$$

Since $y(1) \geq 3$ we deduce that $y > 0$, and so $q^2 > 6f$. $\square$

Now we consider the Case (VII).

Lemma 3.3.10. *Let Ω be a set of size n and let $G \leq \mathrm{Sym}(\Omega)$ be a primitive almost simple group with socle $G_0 = \mathrm{P}\Omega_8^+(q)$. Then*

$$\mathrm{I}(G) < 5\log n - 1.$$

Proof. If $q = 2$, then $|G| \leq 6|G_0| < q^{30}$ by [20, p85]. If $q \geq 3$, then $|G| < 6fq^{28}$ by [28, (6.19)] and so $|G| < q^{30}$ by Lemma 3.3.9.

By Lemmas 2.3.1(ii) and 2.6.5

$$\mathrm{I}(G) \leq \log|G| - 1 < \log q^{30} - 1 = 5\log q^6 - 1.$$

Since $q^6 < n$ by [28, (6.20)], the result then follows. □

We now consider Case (VIII).

Lemma 3.3.11. *Let $d = 2m \geq 10$, let G be a primitive almost simple group with socle $G_0 = \mathrm{P}\Omega_d^+(q)$, let Ω be a G-orbit of $\mathcal{PG}_m(V)$, and let $n = |\Omega|$. Then*

$$\mathrm{I}(G, \Omega) < 5 \log n - 1.$$

Proof. We begin by showing that

$$\frac{d^2}{8} - \frac{d}{4} > \frac{d^2}{10} - \frac{d}{10} + \frac{1}{5}. \tag{3.16}$$

Let $y(d) = d^2 - 6d - 8 = (d - (3 + \sqrt{17}))(d - (3 - \sqrt{17}))$. Since $3+\sqrt{17}, 3-\sqrt{17} < 8$, it follows that $y(d) > 0$ for $d \geq 10$. Therefore $2d^2 - 12d - 16 > 0$ and so $10d^2 - 20d > 8d^2 - 8d + 16$. Hence (3.16) follows by dividing both sides of the previous expression by 80.

Combining (3.16) with [7, Table 4.12] gives

$$n = \prod_{i=1}^{\frac{d}{2}-1} (q^i + 1) > \prod_{i=1}^{\frac{d}{2}-1} q^i = q^{\frac{1}{2}\left(\frac{d}{2}-1\right)\frac{d}{2}} = q^{\frac{d^2}{8} - \frac{d}{4}} > q^{\frac{d^2}{10} - \frac{d}{10} + \frac{1}{5}}. \tag{3.17}$$

Hence

$$\begin{aligned}
\mathrm{I}(G) &< \log |G| - 1 && \text{by Lemmas 2.3.1(ii) and 2.6.5,} \\
&\leq \log \left(q^{\frac{d^2}{2} - \frac{d}{2} + 1} \right) - 1 && \text{by [28, p25],} \\
&= 5 \log \left(q^{\frac{d^2}{10} - \frac{d}{10} + \frac{1}{5}} \right) - 1 && \\
&< 5 \log n - 1 && \text{by (3.17).} \quad \square
\end{aligned}$$

Finally, we consider Case (IX).

Proposition 3.3.12. *Let $d \geq 3$, let $G \leq \mathrm{P}\Gamma\mathrm{L}_d(q)$ be primitive almost simple, and let $\Omega \subseteq \mathcal{PG}_m(V)$ with $n = |\Omega| > q^{\frac{1}{2}m(d-m)}$. Then*

$$\mathrm{I}(G, \Omega) < 5 \log n - 1.$$

Proof. Lemma 2.3.3 implies that

$$\mathrm{I}(G) \leq \mathrm{I}\big(\mathrm{P}\Gamma\mathrm{L}_d(q), \mathcal{PG}_m(V)\big),$$

and so in particular the bounds from Proposition 3.1.3 apply. From $n = |\Omega| > q^{\frac{1}{2}m(d-m)}$ it follows that

$$\frac{1}{2} m(d-m) \log q < \log n. \tag{3.18}$$

We begin with $m = 1$. If $q = 2$, then by Theorem 2.5.2 it follows that $d \geq 4$. First let $d = 4$. Then by Lemma 2.6.5 and Proposition 3.1.3,

$$\mathrm{I}(G) \leq 2(4-1)+1 = 7 < 5\log 5 - 1 \leq 5\log n - 1.$$

Now let $d \geq 5$. Then

$$\begin{aligned}
\mathrm{I}(G) &\leq 2(d-1)+1 && \text{by Proposition 3.1.3,}\\
&\leq 2(d-1)+\tfrac{1}{2}(d-1)-1 && \text{since } d \geq 5,\\
&= \tfrac{5}{2}(d-1)-1 && \\
&< 5\log n - 1 && \text{by (3.18).}
\end{aligned}$$

To complete the case of $m = 1$, let $q \geq 3$. We first show that

$$\log f + 1 < \frac{7}{6}(d-1)\log q - 1. \qquad (3.19)$$

Let $y(f) = 14f - 6\log f - 12$. Then $\frac{dy}{df} = 14 - \frac{6}{f\ln 2}$, and so $\frac{dy}{df} = 0$ if and only if $f = \frac{6}{14\ln(2)} < 1$. Since $\frac{dy}{df}(1) > 0$ it follows that $\frac{dy}{df} > 0$ for all $f \geq 1$. Therefore from $y(1) = 2 > 0$ it follows that $6\log f + 12 < 14f$ for $f \geq 1$. Therefore (3.19) holds since

$$\log f + 2 < \frac{7f}{6}\cdot 2 \leq \frac{7f}{6}(d-1) \leq \frac{7f}{6}(d-1)\log p = \frac{7}{6}(d-1)\log q.$$

Therefore

$$\begin{aligned}
\mathrm{I}(G) &\leq \tfrac{4}{3}(d-1)\log q + \log f + 1 && \text{by Proposition 3.1.3,}\\
&< \tfrac{4}{3}(d-1)\log q + \tfrac{7}{6}(d-1)\log q - 1 && \text{by (3.19),}\\
&= 5\big(\tfrac{1}{2}(d-1)\log q\big) - 1, && \\
&< 5\log n - 1 && \text{by (3.18).}
\end{aligned}$$

Now let $m = \frac{d}{2}$ and $q = 2$. Then

$$\begin{aligned}
\mathrm{I}(G) &\leq \tfrac{d^2}{2} + 1 && \text{by Proposition 3.1.3,}\\
&= 4\big(\tfrac{1}{2}m(d-m)\big) + 1 && \text{since } m = \tfrac{d}{2},\\
&< 4\log n + 1 && \text{by (3.18),}\\
&< 4\log n + \log n - 1 && \text{since } n \geq 5 \text{ by Lemma 2.6.5,}\\
&= 5\log n - 1.
\end{aligned}$$

Finally, we assume that $m > 1$, and that if $m = \frac{d}{2}$, then $q > 2$. Therefore

$$\begin{aligned} \mathrm{I}(G) &\leq 2m(d-m)\log q + \log f && \text{by Proposition 3.1.3,} \\ &\leq 2m(d-m)\log q + \tfrac{1}{3}m(d-m)\log q - \tfrac{4}{3} && \text{by Lemma 3.3.5,} \\ &= \tfrac{7}{3}m(d-m)\log q - \tfrac{4}{3} \\ &< \tfrac{14}{3}\log n - \tfrac{4}{3} && \text{by (3.18),} \\ &< 5\log n - 1. \quad \square \end{aligned}$$

We finish this section by proving Theorem 3.3.1.

Proof of Theorem 3.3.1. We proceed through the Cases (I)-(IX) of Lemma 2.7.14. If G is as in Case (I) in the result holds by Lemma 3.3.2. Let G be as in Case (II). Since G is not large base it follows that Ω is a set of partitions, and so $\mathrm{I}(G,\Omega) < 2\log|\Omega|$ by [28, Lemma 6.6]. If G is as in Case (III), then the result holds by Proposition 3.3.6. If G is as in Case (IV) or (V), then the result holds by Lemma 3.3.8. If G is as in Case (VI), then $\mathrm{I}(G,\Omega) < \frac{11}{3}\log|\Omega|$ by [28, Lemma 6.7]. If G is as in Case (VII), then the result holds by Lemma 3.3.10. If G is as in Case (VIII), then the result holds by Lemma 3.3.11. If G is as in Case (IX), then the result holds by Proposition 3.3.12 □

3.4 Proof of Theorems 3.0.3 and 3.0.4

To prove Theorem 3.0.3 we divide into the eight cases of the O'Nan Scott Theorem - HA, TW, HS, HC, AS, SD, CD and PA. Using the following result of Gill, Loda and Spiga, it remains to consider type PA.

Theorem 3.4.1. *[28, Propositions 3.1, 4.1 and 5.1] Let G be a permutation group on a finite set Ω of size n.*

(i) *If G contains a regular normal subgroup, and so in particular if G is of type HA, TW, HS or HC, then* $\mathrm{I}(G) \leq \log n + 1$.

(ii) *If G is a primitive group of type SD, then* $\mathrm{I}(G) \leq \log n$.

(iii) *If G is a primitive group of type CD, then* $\mathrm{I}(G) < 2\log n$.

We now consider groups of type PA.

Lemma 3.4.2. *Let G be a primitive subgroup of S_n of type PA that is not large base. Then*

$$\mathrm{I}(G) < 5\log n.$$

Proof. Since G is of type PA there exists an integer $r \geq 2$, a finite set Δ and an almost simple subgroup H of $\mathrm{Sym}(\Delta)$ such that $G \leq H \operatorname{wr} \mathrm{S}_r$. By Lemma 2.6.6, H is not large base. Let $s = |\Delta|$. Then $n = s^r$, and $s \geq 5$ by Lemma 2.6.5. Therefore

$$\begin{aligned}
\mathrm{I}(G,\Omega) &\leq \mathrm{I}(H^r,\Delta^r) + \ell(\mathrm{S}_r) && \text{by Lemmas 2.3.3 and 2.3.5,}\\
&\leq \mathrm{I}(H^r,\Delta^r) + \tfrac{3}{2}r && \text{by Theorem 2.2.8,}\\
&\leq r(\mathrm{I}(H,\Delta)-1) + 1 + \tfrac{3}{2}r && \text{by Lemma 2.3.4,}\\
&< r(5\log s - 2) + 1 + \tfrac{3}{2}r && \text{by Theorem 3.3.1,}\\
&< 5\log s^r - \tfrac{1}{2}r + 1 && \\
&\leq 5\log n && \text{since } r \geq 2. \quad \square
\end{aligned}$$

We can now prove Theorem 3.0.3.

Proof of Theorem 3.0.3. Let G be a primitive group which is not large base. If G is almost simple, then the result holds by Theorem 3.3.1. If G is of type PA, then the result holds by Lemma 3.4.2. For the remaining cases of the O'Nan-Scott Theorem, the result holds by Theorem 3.4.1. □

Finally, we prove Theorem 3.0.4.

Proof of Theorem 3.0.4. Let $\mathbb{F} = \mathrm{GF}(2)$, let $m \geq 3$, let $d = 2m+2$, let $V = \mathbb{F}^d$, let $G = \mathrm{PGL}_d(2) = \mathrm{PSL}_d(2) = \mathrm{GL}_d(2)$ act on $\Omega = \mathcal{PG}_m(V)$, and let $n = |\Omega|$. We show that

$$\mathrm{I}(G) > \frac{8}{63}\mathrm{b}(G)\log n,$$

from which the result will follow.

We begin by finding an upper bound on $\log n$. By Lemma 2.7.2

$$\begin{aligned}
n &= \frac{(2^{2m+2}-1)(2^{2m+1}-1)\cdots(2^{m+3}-1)}{(2^m-1)(2^{m-1}-1)\cdots(2-1)}\\
&< \frac{2^{(2m+2)+(2m+1)+\cdots+(m+3)}}{2^{(m-1)+(m-2)+\cdots+1+0}}.
\end{aligned}$$

Hence

$$\begin{aligned}
\log n &< \frac{1}{2}(2m+2)(2m+3) - \frac{1}{2}(m+2)(m+3) - \frac{1}{2}(m-1)m\\
&= \frac{1}{2}(4m^2+10m+6-m^2-5m-6-m^2+m)\\
&= \frac{1}{2}(2m^2+6m)\\
&= m^2+3m.
\end{aligned}$$

Therefore by Theorem 3.1.2

$$\mathrm{I}(G) \geq m^2+2m+1 > \frac{m^2+2m+1}{m^2+3m}\log n = \Big(1 - \frac{m-1}{m^2+3m}\Big)\log n.$$

Let $f(m) = \frac{m-1}{m^2+3m}$. Then f tends to zero as m tends to infinity. We now find the maximum value of $f(m)$ over $m \geq 3$. From

$$\frac{df}{dm} = \frac{1(m^2+3m)-(m-1)(2m+3)}{(m^2+3m)^2} = \frac{-m^2+2m+3}{(m^2+3m)^2} = \frac{-(m+1)(m-3)}{(m^2+3m)^2},$$

it follows that $\frac{df}{dm} = 0$ if and only if $(m+1)(m-3) = 0$. Hence f has two critical points at $m = -1$ and $m = 3$. Now $f(3) = \frac{1}{9} > \frac{3}{28} = f(4)$, and so it follows that $f(m) \leq \frac{1}{9}$ for $m \geq 3$. Therefore

$$\mathrm{I}(G) > \left(1 - \frac{1}{9}\right) \log n = \frac{8}{9} \log n.$$

By [30, p7]

$$\mathrm{b}(G) \leq \frac{d}{m} + 5 = \frac{2m+2}{m} + 5 = 7 + \frac{2}{m} < 8,$$

and so $\mathrm{b}(G) \leq 7$. Hence

$$\mathrm{I}(G) > \frac{1}{7}\mathrm{b}(G) \cdot \frac{8}{9} \log n = \frac{8}{63}\mathrm{b}(G) \log n. \quad \square$$

Chapter 4

Maximal subgroups and maximal cocliques

4.1 Intransitive and imprimitive groups

In this section we introduce two families of maximal subgroups of $\mathrm{S}_n := \mathrm{Sym}(\{1, \ldots, n\})$ and $\mathrm{A}_n := \mathrm{Alt}(\{1, \ldots, n\})$, these groups will be our main focus in Chapters 5 and 6. We begin by defining the imprimitive action of a wreath product.

Recall the definition of a wreath product given in Section 2.1.1 (here we use R in place of K). Let H and R be finite groups acting on finite sets $\Delta = \{1, \ldots, k\}$ and $\Gamma = \{1, \ldots, m\}$ respectively. For $\delta \in \Delta$ and $\gamma \in \Gamma$ let δ^h and γ^r denote the images of δ and γ under $h \in H$ and $r \in R$ respectively. Let $\phi : R \to \mathrm{Aut}(H^m)$ where

$$\phi(r) : (h_1, \ldots, h_m) \mapsto (h_{1^{r^{-1}}}, \ldots, h_{m^{r^{-1}}}),$$

and let $G = H \operatorname{wr} R = H \rtimes_\phi R$.

The *imprimitive action* of G on $\Omega = \Delta \times \Gamma$ is as follows. Let $(\delta, \gamma) \in \Omega$, let $g = \Big((h_1, \ldots, h_m), r\Big) \in G$, and let h_γ be the γ^{th} coordinate of $(h_1, \ldots, h_m)$. Then the image of (δ, γ) under g is

$$(\delta^{h_\gamma}, \gamma^r).$$

Example 4.1.1. Let $\Delta = \{1, 2, 3\}$ and $\Gamma = \{1, 2, 3, 4\}$, let $H = \mathrm{Sym}(\Delta) \cong \mathrm{S}_3$ and $R = \mathrm{Sym}(\Gamma) \cong \mathrm{S}_4$, and let $G = H \operatorname{wr} R$. Then G acts on $\Omega = \Delta \times \Gamma$ via the imprimitive action. For example let

$$g = \big((h_1, h_2, h_3, h_4), r\big) = \Bigg(\Big((1,2), (1,2,3), (2,3), (1,3,2)\Big), (1,4)(2,3)\Bigg) \in G.$$

Then g acts on the points of Ω as follows.

$$\begin{array}{lll}
(1,1)^g=(1^{h_1},1^r)=(2,4) & (2,1)^g=(2^{h_1},1^r)=(1,4) & (3,1)^g=(3^{h_1},1^r)=(3,4)\\
(1,2)^g=(1^{h_2},2^r)=(2,3) & (2,2)^g=(2^{h_2},2^r)=(3,3) & (3,2)^g=(3^{h_2},2^r)=(1,3)\\
(1,3)^g=(1^{h_3},3^r)=(1,2) & (2,3)^g=(2^{h_3},3^r)=(3,2) & (3,3)^g=(3^{h_3},3^r)=(2,2)\\
(1,4)^g=(1^{h_4},4^r)=(3,1) & (2,4)^g=(2^{h_4},4^r)=(1,1) & (3,4)^g=(3^{h_4},4^r)=(2,1) \quad \triangle
\end{array}$$

Let $\Delta = \{1,\dots,k\}$, let $\Gamma = \{1,\dots,m\}$, let $H \leq \mathrm{S}_k$, let $R \leq \mathrm{S}_m$, and let $G = H \operatorname{wr} R \leq \mathrm{S}_k \operatorname{wr} \mathrm{S}_m$. Then G acts on $\{1,\dots,k\} \times \{1,\dots,m\}$ with imprimitive action.

Let $f : \{1,\dots,k\} \times \{1,\dots,m\} \to \{1,\dots,mk\}$ with $(i,j) \mapsto i + k(j-1)$. It is easily seen that f is a bijection and that using f the action of G on $\{1,\dots,k\} \times \{1,\dots,m\}$ is equivalent to the action of G on $\{1,\dots,mk\}$.

Example 4.1.2. Let G and g be as in Example 4.1.1. Let

$$f : \{1,\dots,3\} \times \{1,\dots,4\} \to \{1,\dots,12\} \text{ with } (i,j) \mapsto i + 3(j-1).$$

The element of $\mathrm{Sym}(\{1,\dots,3\} \times \{1,\dots,4\})$ induced by g is

$$\Big((1,1),(2,4)\Big)\Big((2,1),(1,4),(3,1),(3,4)\Big)\Big((1,2),(2,3),(3,2),(1,3)\Big)\Big((2,2),(3,3)\Big),$$

and the element of $\mathrm{Sym}(\{1,\dots,12\})$ induced by g is

$$(1,11)(2,10,3,12)(4,8,6,7)(5,9). \quad \triangle$$

For the remainder of this section we use the following notation. Since we never use (i) and (ii) simultaneously and the context is always made clear, there will be no confusion between the different set ups.

Notation 4.1.3. Let $\Omega = \{1,\dots,n\}$ and let $\mathrm{S}_n = \mathrm{Sym}(\Omega)$ and let $H \leq \mathrm{S}_n$.

(i) If H is intransitive, then there exist non-empty sets $\Omega_1, \Omega_2 \subseteq \Omega$ such that $\Omega = \Omega_1 \dot\cup \Omega_2$ and $H \leq \mathrm{Sym}(\Omega_1) \times \mathrm{Sym}(\Omega_2)$. Up to conjugation in S_n we may let $\Omega_1 = \{1,\dots,k\}$ and $\Omega_2 = \{k+1,\dots,n\}$ with $\frac{n}{2} \leq k \leq n-1$. Then

$$H \leq \mathrm{Sym}(\{1,\dots,k\}) \times \mathrm{Sym}(\{k+1,\dots,n\}) \cong \mathrm{S}_k \times \mathrm{S}_{n-k}.$$

(ii) If H is imprimitive, then H preserves some non-trivial block system, say $\{\Omega_1,\dots,\Omega_m\}$ with block size k. Then $m,k \geq 2$. Up to conjugation in S_n we may let

$$\Omega_1 = \{1,2,\dots,k\},\ \Omega_2 = \{k+1,\dots,2k\},\ \dots\ ,\ \Omega_m = \{(m-1)k+1,\dots,mk\}.$$

Then $H \leq \mathrm{S}_k \operatorname{wr} \mathrm{S}_m$.

Lemma 4.1.4. *[39, Theorem 1] Let $G = \mathrm{S}_n$ or A_n.*

(i) *Let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$. Then M is maximal in G when $k \neq n-k$.*

(ii) *Let $M = (\mathrm{S}_k \operatorname{wr} \mathrm{S}_m) \cap G$ with $n = mk$ and $m, k \geq 2$. Then M is maximal in G unless $(G, k) = (\mathrm{A}_8, 2)$.*

In the following let $g \in \mathrm{S}_n$ act on Ω^k coordinate-wise.

Definition 4.1.5. (i) Let $G \leq \mathrm{S}_k \times \mathrm{S}_{n-k}$ with the natural intransitive action on $\Omega = \Omega_1 \dot\cup \Omega_2$. Then G is (t_1, t_2)*-transitive* on $\Omega_1 \dot\cup \Omega_2$ if for all sequences of distinct points $U, V \in \Omega_1^{t_1} \times \Omega_2^{t_2}$ there exists $g \in G$ with $U^g = V$.

(ii) Let $G \leq \mathrm{S}_k \operatorname{wr} \mathrm{S}_m$ with the natural imprimitive action on $\Omega = \Omega_1 \dot\cup \cdots \dot\cup \Omega_m$. Then G is $\{t_1, t_2, \ldots, t_m\}$*-transitive* on $\Omega_1 \dot\cup \Omega_2 \dot\cup \cdots \dot\cup \Omega_m$ if for all tuples of distinct points $(U_1, \ldots, U_m) \in (\Omega_{a_1}^{t_1}, \ldots, \Omega_{a_m}^{t_m})$ and $(V_1, \ldots, V_m) \in (\Omega_{b_1}^{t_1}, \ldots, \Omega_{b_m}^{t_m})$ such that $\{a_1, \ldots, a_m\} = \{1, \ldots, m\} = \{b_1, \ldots, b_m\}$, there exists $g \in G$ such that $(U_1, \ldots, U_m)^g = (V_1, \ldots, V_m)$.

In the following example we illustrate the notation given above.

Example 4.1.6. (i) Let $G = \mathrm{S}_5 \times \mathrm{S}_3$ with natural intransitive action on $\Omega_1 \cup \Omega_2 = \{1,2,3,4,5\} \cup \{6,7,8\}$, and let

$$U = \big((1,2,3,4,5),(6,8)\big),\ V = \big((3,5,4,1,2),(7,8)\big) \in \Omega_1^5 \times \Omega_2^2.$$

Then $g = (1,3,4)(2,5)(6,7) \in G$ with $U^g = V$.

(ii) Let $G = \mathrm{S}_3 \operatorname{wr} \mathrm{S}_3$ with natural imprimitive action on

$$\Omega = \Omega_1 \dot\cup \Omega_2 \dot\cup \Omega_3 = \{1,2,3\} \dot\cup \{4,5,6\} \dot\cup \{7,8,9\}.$$

Let

$$(U_1, U_2, U_3) = \big((1,2),(4,5,6),(9)\big) \in (\Omega_1^2, \Omega_2^3, \Omega_3^1)$$

and let

$$(V_1, V_2, V_3) = \big((4,6),(9,7,8),(2)\big) \in (\Omega_2^2, \Omega_3^3, \Omega_1^1).$$

Then $g = (1,4,9,2,6,8,3,5,7) \in G$ with $(U_1, U_2, U_3)^g = (V_1, V_2, V_3)$. △

We now prove a crucial lemma about (t_1, t_2)-transitive intransitive groups.

Lemma 4.1.7. *Let $n \geq 5$, let $\frac{n}{2} < k < n$, let $\Omega = \Omega_1 \dot\cup \Omega_2 = \{1, \ldots, k\} \cup \{k+1, \ldots, n\}$, let $G = \mathrm{S}_n$ or A_n, and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$.*

(i) *If $G = \mathrm{S}_n$, then M is $(k, n-k)$-transitive on $\Omega_1 \dot\cup \Omega_2$.*

(ii) *If $G = \mathrm{A}_n$, then:*

(a) *M is $(k-2, n-k)$-transitive on $\Omega_1 \dot\cup \Omega_2$,*

(b) *if $n-k \geq 3$, then M is $(k, n-k-2)$-transitive on $\Omega_1 \dot\cup \Omega_2$.*

Proof. Part (i) is immediate since S_t is t-transitive.

For Part (ii)(a) let $U, V \in \Omega_1^{k-2} \times \Omega_2^{n-k}$ be tuples of distinct points. Then there exist $\alpha, \beta \in \Omega_1$ such that α, β are distinct and not entries of U. By (i) there exists $h \in \mathrm{S}_k \times \mathrm{S}_{n-k}$ such that $h(u_i) = v_i$ for $1 \leq i \leq n-2$. Then G contains either h or $(\alpha, \beta)h$.

Part (ii)(b) follows by symmetry. □

We now prove an important lemma about transitivity of imprimitive groups.

Lemma 4.1.8. *Let $m, k \geq 2$, let $n = mk$, let $\Omega_i = \{(i-1)k+1, \dots, ik\}$ for $1 \leq i \leq m$, let $G = \mathrm{S}_n$ or A_n, and let $M = (\mathrm{S}_k \operatorname{wr} \mathrm{S}_m) \cap G$.*

(i) *If $G = \mathrm{S}_n$, then M is $\{k, k, \dots, k\}$-transitive on $\Omega_1 \dot\cup \Omega_2 \dot\cup \cdots \dot\cup \Omega_m$.*

(ii) *If $G = \mathrm{A}_n$, then M is $\{k, \dots, k, k-2\}$-transitive on $\Omega_1 \dot\cup \Omega_2 \dot\cup \cdots \dot\cup \Omega_m$.*

Proof. Let $(U_1, \dots, U_m) \in (\Omega_{a_1}^k, \dots, \Omega_{a_m}^k)$ and $(V_1, \dots, V_m) \in (\Omega_{b_1}^k, \dots, \Omega_{b_m}^k)$ be tuples of distinct points such that $\{a_1, \dots, a_m\} = \{1, \dots, m\} = \{b_1, \dots, b_m\}$.

Since S_n is n-transitive there exists $g \in \mathrm{S}_n$ such that $(U_1, \dots, U_m)^g = (V_1, \dots, V_m)$. From $U_i^g = V_i$ it follows that $\Omega_{a_i}^g = \Omega_{b_i}$ for $1 \leq i \leq m$, and so $g \in M$. Hence Part (i) follows.

For Part (ii) let $U_i \in \Omega_{a_i}^k$, $V_i \in \Omega_{b_i}^k$ for $1 \leq i \leq m-1$ and $U_m \in \Omega_{a_m}^{k-2}$, $V_m \in \Omega_{b_m}^{k-2}$ be tuples of distinct points such that $\{a_1, \dots, a_m\} = \{1, \dots, m\} = \{b_1, \dots, b_m\}$.

Let α, β be the two points of Ω_{a_m} not contained in U_m. By Part (i) there exists $h \in \mathrm{Sym}(k) \operatorname{wr} \mathrm{Sym}(m)$ such that $U_i^h = V_i$ for $1 \leq i \leq m$. Then G contains either h or $(\alpha, \beta)h$. □

4.2 Block systems and cycle structures

In this section we first cover some notation and lemmas on the cycle structure of elements of S_n. We then reintroduce block systems (which we defined in Section 2.1.3) and give some more notation. We then consider the interaction between cycle structures and block systems. We prove various results which limit the possible block systems for groups with certain properties. This will be used in Chapters 5 and 6 when proving that the groups we generate are primitive.

4.2.1 Cycle Structures

We begin with cycle structures.

Lemma 4.2.1. *Let $y \in \mathrm{S}_n$ and let t be the number of cycles in the disjoint cycle decomposition of y (including trivial cycles). Then y is even if and only if t and n have the same parity.*

Proof. Let y have t_1 cycles of odd length and t_2 cycles of even length, so that $t_1 + t_2 = t$. Then $n \equiv t_1 \bmod 2$, and so

$$t - n \equiv t - t_1 = t_2 \bmod 2.$$

Hence t and n have the same parity if and only if t_2 is even, that is if and only if y is even. □

For an element of S_n we use the following notation for cycle type and support.

Notation 4.2.2. Let $y \in \mathrm{S}_n$ with disjoint cycle decomposition $c_1, \ldots, c_t$ (including trivial cycles). For $1 \leq i \leq t$, let $\Theta_i = \mathrm{Supp}(c_i)$ and let $l(c_i)$ be the length of c_i. We denote the cycle type of y by $\mathcal{C}(y) = l(c_1) \cdot l(c_2) \cdot \cdots \cdot l(c_t)$. The "$\cdot$" notation is omitted when it is clear without, and we sometimes gather together common cycle orders and use the usual exponent notation.

For example if $y = (1,2,3)(4,5)(6,7)$, then we may let $c_1 = (1,2,3)$, $c_2 = (4,5)$ and $c_3 = (6,7)$. Thus $\Theta_1 = \{1,2,3\}$, $\Theta_2 = \{4,5\}$ and $\Theta_3 = \{6,7\}$, and we may choose to write $\mathcal{C}(y) = 3 \cdot 2 \cdot 2$ or $\mathcal{C}(y) = 3 \cdot 2^2$.

The next lemma guarantees the existence of certain sets of distinct points in the support of an element of S_n. We make use of this result for a small number of cases in Chapter 5 when constructing transitive groups.

Lemma 4.2.3. *Let $k, n \in \mathbb{N}$ with $\frac{n}{2} < k < n$, and let $x \in \mathrm{S}_n$ be such that $1^x = k+1$.*

(i) *If $|\mathrm{Supp}(x)| \geq 8$ and x does not have cycle type $1^{(n-8)} \cdot 2 \cdot 3^2$, $1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-9)} \cdot 3^3$, then there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x \in \mathrm{Supp}(x) \backslash \{1, k+1\}$.*

(ii) *If $|\mathrm{Supp}(x)| \geq 8$ and x does not have cycle type $1^{(n-8)} \cdot 2^4$, then there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \delta, \epsilon \in \mathrm{Supp}(x) \backslash \{1, k+1\}$ such that (δ, ϵ) is not a cycle of x.*

Proof. Let $T = \mathrm{Supp}(x) \backslash 1^{\langle x \rangle}$. We split into cases based on $|1^{\langle x \rangle}|$.

(i) If $|1^{\langle x \rangle}| \geq 8$, then we may let $\alpha = 1^{x^2}, \beta = 1^{x^4}$ and $\gamma = 1^{x^6}$. If $6 \leq |1^{\langle x \rangle}| \leq 7$, then $|T| \geq 2$, and so we may $\alpha = 1^{x^2}$, $\beta = 1^{x^4}$ and let $\gamma \in T$.

If $4 \leq |1^{\langle x \rangle}| \leq 5$, then $|T| \geq 4$ because x does not have cycle type $1^{(n-8)} \cdot 3 \cdot 5$. Then $\langle x \rangle$ has either at least two orbits on T of size at least 2; or at least one orbit of size at least 4. Therefore, we may let $\alpha = 1^{x^2}$ and $\beta, \gamma \in T$.

If $|1^{\langle x \rangle}| \leq 3$, then $|T| \geq 6$ because the cycle type of x is neither $1^{(n-8)} \cdot 3 \cdot 5$ nor $1^{(n-8)} \cdot 2 \cdot 3^2$. If $\langle x \rangle$ has one orbit on T, then the orbit has size at least 6. If $\langle x \rangle$ has two orbits on T, then since x does not have cycle type $1^{(n-9)} \cdot 2 \cdot 3^2$ or $1^{(n-9)} \cdot 3^3$, it follows that these have sizes at least 3 and 4. Otherwise $\langle x \rangle$ has at least three orbits on T of size at least 2. Therefore, we may let $\alpha, \beta, \gamma \in T$.

(ii) If $|1^{\langle x \rangle}| \geq 8$, then let $\delta = 1^{x^2}$, $\epsilon = 1^{x^3}$, $\alpha = 1^{x^4}$ and $\beta = 1^{x^6}$. If $6 \leq |1^{\langle x \rangle}| \leq 7$, then $|T| \geq 2$, and so let $\delta = 1^{x^2}$, $\epsilon = 1^{x^3}$, $\alpha = 1^{x^4}$ and let $\beta \in T$. If $|1^{\langle x \rangle}| = 5$, then $|T| \geq 3$, so let $\alpha, \alpha^x, \delta \in |1^{\langle x \rangle}|$ and $\beta, \beta^x, \epsilon \in T$. If $|1^{\langle x \rangle}| = 4$, then $|T| \geq 4$, so let $\delta, \epsilon \in |1^{\langle x \rangle}|$ and $\alpha, \alpha^x, \beta, \beta^x \in T$. If $|1^{\langle x \rangle}| = 3$, then $|T| \geq 5$ and we may let $\delta \in 1^{\langle x \rangle}$ and $\beta, \beta^x, \alpha, \alpha^x, \epsilon \in T$. Finally suppose that $|1^{\langle x \rangle}| = 2$, and so $|T| \geq 6$. Since the cycle type of x is not $1^{(n-8)} \cdot 2^4$, we may let $\alpha, \alpha^x, \beta, \beta^x, \delta, \epsilon \in T$. □

4.2.2 Block Systems

We now turn our attention to block systems. We begin by repeating Definition 2.1.9 below.

Definition 4.2.4. Let G be a transitive subgroup of $\mathrm{Sym}(\Omega)$. A set $\Delta \subseteq \Omega$ is a *block* for G if for all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$.

Let Δ be a block. If $|\Delta| = 1$ or $\Delta = \Omega$, then Δ is a *trivial* block; otherwise Δ is *non-trivial.*

Definition 4.2.5. Let G be a transitive group with a block Δ. Then

$$\Sigma = \{\Delta^g \mid g \in G\}$$

is a *block system* for G. If Δ is trivial, then Σ is a *trivial* block system; otherwise Σ is a *non-trivial* block system.

Lemma 4.2.6. *Let G be a transitive subgroup of* $\mathrm{Sym}(\Omega)$ *with block Δ. Then $|\Delta|$ divides $|\Omega|$.*

Proof. It follows from the definition of a block and transitivity that a block system forms a partition of Ω. Since $|\Delta| = |\Delta^g|$ for $g \in G$, the result follows. □

Definition 4.2.7. Let Δ be a non-trivial block. If Δ is contained in no larger non-trivial block, then Δ is a *maximal* block. If Δ contains no smaller non-trivial block, then Δ is a *minimal* block.

Recall by Definition 2.1.9 that a transitive group G is primitive if it has no non-trivial blocks, and otherwise is imprimitive.

4.2.3 Interactions between Cycle Structures and Block Systems

We now consider the interaction between cycle structures and block systems. For the rest of this section, and in Chapters 5 and 6, we use the following notation for two block systems preserved by different groups acting on the same set.

Notation 4.2.8. Let $\Omega = \{1, \dots, n\}$, let $G = \mathrm{Sym}(\Omega) = \mathrm{S}_n$, let M be a maximal imprimitive subgroup of G with unique non-trivial block system $\mathcal{M}$, and let H be a transitive subgroup of G with (possibly trivial) block system $\mathcal{H}$.

If the blocks of $\mathcal{H}$ have size at least 2, then we say that $\mathcal{H}$ is a *non-singelton* block system. We call elements of $\mathcal{H}$ and $\mathcal{M}$ the *H-blocks* and *M-blocks* respectively. For $\alpha \in \Omega$, let $\Omega(\alpha)$ and $\Delta(\alpha)$ denote the M and H-block containing α.

Let $h \in H$ and let h_i be a cycle of h. Then $h_i^{\mathcal{H}}$ denotes the permutation that h induces on the set of blocks in $\mathcal{H}$ which contain points of $\mathrm{Supp}(h_i)$. Similarly, for $g \in M$ with cycle g_i we let $g_i^{\mathcal{M}}$ denote the permutation that g induces on the blocks of $\mathcal{M}$ which contain points of $\mathrm{Supp}(g_i)$. Let $g^{\mathcal{M}}$ be the permutation that g induces on the blocks of $\mathcal{M}$.

In the following example we use the same notation as in Examples 4.1.1 and 4.1.2.

Example 4.2.9. Let $G = \mathrm{S}_{12}$ and let $M = \mathrm{S}_3 \operatorname{wr} \mathrm{S}_4$. Then

$$\mathcal{M} = \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\} = \big\{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{10,11,12\}\big\}$$

and $\Omega(3) = \Omega_1$. Let

$$g = g_1 g_2 g_3 g_4 = (1, 11)(2, 10, 3, 12)(4, 8, 6, 7)(5, 9) \in M.$$

Then $g_1^{\mathcal{M}} = g_2^{\mathcal{M}} = (\Omega_1, \Omega_4)$ and $g_3^{\mathcal{M}} = g_4^{\mathcal{M}} = (\Omega_2, \Omega_3)$.

Observe that $g^{\mathcal{M}} = (\Omega_1, \Omega_4)(\Omega_2, \Omega_3)$, which corresponds to r in Example 4.1.1. △

Lemma 4.2.10. *Let H be a transitive group with block system $\mathcal{H}$ and let $h \in H$ with h_i a cycle of h. Then $h_i^{\mathcal{H}}$ is a cycle whose length divides the length of h_i.*

Proof. Since h_i is transitive on the points of $\mathrm{Supp}(h_i)$, it follows that $h_i^{\mathcal{H}}$ is a cycle. Let Δ be a block containing $m > 0$ points of $\mathrm{Supp}(h_i)$. By taking h_i translates of Δ, we deduce that each block of $\mathcal{H}$ contains exactly m or 0 points of $\mathrm{Supp}(h_i)$. Hence $|h_i| = m|h_i^{\mathcal{H}}|$. □

The next two lemmas will be used in Chapters 5 and 6. The following considers the interaction between block systems and induced cycles.

Lemma 4.2.11. *Let H be a transitive group with block system $\mathcal{H}$, let $\Delta \in \mathcal{H}$, let $h \in H$, and let h_1 and h_2 be (possibly trivial) cycles of h.*

(i) *If $\Delta \in \mathrm{Supp}(h_1^{\mathcal{H}}) \cap \mathrm{Supp}(h_2^{\mathcal{H}})$, then $h_1^{\mathcal{H}} = h_2^{\mathcal{H}}$.*

(ii) *If h_1 has prime length p, then the points of $\mathrm{Supp}(h_1)$ are either all in the same block or all in different blocks.*

(iii) *Suppose that h_1 and h_2 have coprime lengths. If $\Delta \in \mathrm{Supp}(h_1^{\mathcal{H}}) \cap \mathrm{Supp}(h_2^{\mathcal{H}})$, then $\mathrm{Supp}(h_1) \cup \mathrm{Supp}(h_2) \subseteq \Delta$.*

(iv) *If $l(h_1^{\mathcal{H}}) \nmid l(h_2)$ and $\Delta \in \mathrm{Supp}(h_1^{\mathcal{H}})$, then $\Delta \cap \mathrm{Supp}(h_2) = \emptyset$.*

Proof. (i) If $\Delta \in \mathrm{Supp}(h_1^{\mathcal{H}}) \cap \mathrm{Supp}(h_2^{\mathcal{H}})$, then there exist $\alpha, \beta \in \Delta$ such that $\alpha \in \mathrm{Supp}(h_1)$ and $\beta \in \mathrm{Supp}(h_2)$. Let $i \in \mathbb{N}$. Then since $\alpha, \beta \in \Delta$, it follows that α^{h^i} and β^{h^i} lie in the same block Δ^{h^i}. From $\alpha^{h^i} = \alpha^{h_1^i}$ and $\beta^{h^i} = \beta^{h_2^i}$, it follows that $\Delta^{h_1^i} = \Delta^{h^i} = \Delta^{h_2^i}$, and so $h_1^{\mathcal{H}} = h_2^{\mathcal{H}}$.

(ii) By Lemma 4.2.10, $h_1^{\mathcal{H}}$ is either a p-cycle or a 1-cycle.

(iii) By Part (i), if $\Delta \in \mathrm{Supp}(h_1^{\mathcal{H}}) \cap \mathrm{Supp}(h_2^{\mathcal{H}})$, then $h_1^{\mathcal{H}} = h_2^{\mathcal{H}}$. Since h_1 and h_2 have coprime lengths, it follows from Lemma 4.2.10 that $h_1^{\mathcal{H}}$ is trivial.

(iv) If $\Delta \cap \mathrm{Supp}(h_2) \neq \emptyset$, then $h_1^{\mathcal{H}} = h_2^{\mathcal{H}}$ by Part (i). Hence in particular, $l(h_1^{\mathcal{H}}) = l(h_2^{\mathcal{H}})$. By Lemma 4.2.10 it follows that $l(h_2^{\mathcal{H}}) \mid l(h_2)$ and so $l(h_1^{\mathcal{H}}) \mid l(h_2)$, a contradiction. □

Lemma 4.2.12. *Let $\mathcal{H}$ be a non-singleton block system for H and let $h \in H$ with disjoint cycle decomposition $h_1 \cdots h_t$. If $l(h_i)$ is prime and $\gcd\big(l(h_i), l(h_j)\big) = 1$ for $j \neq i$, then there exists a block $\Delta \in \mathcal{H}$ such that $\mathrm{Supp}(h_i) \subseteq \Delta$. In particular, $\Delta^h = \Delta$.*

Proof. Let Δ be a block containing $\alpha \in \mathrm{Supp}(h_i)$, and let $\beta \in \Delta \backslash \{\alpha\}$. If $\beta \notin \mathrm{Supp}(h)$, then $\beta^h = \beta$, and so $\Delta^h = \Delta$. Hence $\alpha^{\langle h \rangle} = \mathrm{Supp}(h_i) \subseteq \Delta$. Therefore assume that $\beta \in \mathrm{Supp}(h)$. If $\beta \in \mathrm{Supp}(h_i)$, then the result follows by Lemma 4.2.11(ii). If $\beta \notin \mathrm{Supp}(h_i)$, then $\mathrm{Supp}(h_i) \subseteq \Delta$ by Lemma 4.2.11(iii). □

The remainder of this section covers results we will use repeatedly in Chapter 6. The following shows how the support of a cycle can be split across H-blocks and M-blocks.

Lemma 4.2.13. *Let $t \in \mathbb{N}$, let $G = \mathrm{S}_n$ or A_n, let M, H, $\mathcal{M}$ and $\mathcal{H}$ be as in Notation 4.2.8, let $\Omega_1, \ldots, \Omega_t \in \mathcal{M}$, let $\Delta \in \mathcal{H}$, let $y \in M \cap H$ and let c be a cycle of y such that $c^{\mathcal{M}} = (\Omega_1, \ldots, \Omega_t)$ and $\gamma \in \Delta \cap \Omega_1 \cap \mathrm{Supp}(c)$.*

(i) *If* $l(c^{\mathcal{H}}) = t$*, then* $\Delta \cap \mathrm{Supp}(c) = \Omega_1 \cap \mathrm{Supp}(c)$*.*

(ii) *If* $l(c^{\mathcal{H}})$ *divides* t*, then* $\Omega_1 \cap \mathrm{Supp}(c) \subseteq \Delta \cap \mathrm{Supp}(c)$*.*

(iii) *If* $l(c^{\mathcal{H}})$ *is a multiple of* t*, then* $\Delta \cap \mathrm{Supp}(c) \subseteq \Omega_1 \cap \mathrm{Supp}(c)$*.*

(iv) *If* $l(c^{\mathcal{H}}) = l(c)/t$ *and* $\gcd\left(t, \frac{l(c)}{t}\right) = 1$*, then* $|\Delta \cap \mathrm{Supp}(c) \cap \Omega_i| = 1$ *for* $1 \le i \le t$*.*

(v) *If* $l(c^{\mathcal{H}})$ *divides* $l(c)/t$ *and* $\gcd\left(t, \frac{l(c)}{t}\right) = 1$*, then* $|\Delta \cap \mathrm{Supp}(c) \cap \Omega_i| \ge 1$ *for* $1 \le i \le t$*.*

(vi) *If* $l(c^{\mathcal{H}})$ *is a multiple of* $l(c)/t$ *and* $\gcd\left(t, \frac{l(c)}{t}\right) = 1$*, then* $|\Delta \cap \mathrm{Supp}(c) \cap \Omega_i| \le 1$ *for* $1 \le i \le t$*.*

Proof. Let $u, v \in \mathbb{N}$, then

$$\gamma^{\langle y^{uv} \rangle} \subseteq \gamma^{\langle y^u \rangle}. \tag{4.1}$$

Observe that $\gamma^{\langle y^{l(c^{\mathcal{H}})} \rangle} = \Delta \cap \mathrm{Supp}(c)$ and $\gamma^{\langle y^t \rangle} = \Omega_1 \cap \mathrm{Supp}(c)$. Hence Part (i) follows, and so Parts (ii) and (iii) follow by (4.1).

Let $s := l(c)/t$. Assume that $l(c^{\mathcal{H}}) = s$ and that there exist (not necessarily distinct) $\beta, \gamma \in \Omega$ and $1 \le i \le t$ such that $\beta, \gamma \in \Delta \cap \Omega_i \cap \mathrm{Supp}(c)$. From $\beta, \gamma \in \Omega_i$ it follows that there exists an integer $1 \le a \le s$ such that $\beta^{c^{at}} = \gamma$. From $\beta, \gamma \in \Delta$ it follows that there exists an integer $1 \le b \le t$ such that $\beta^{c^{bs}} = \gamma$. Therefore $\beta^{c^{at}} = \beta^{c^{bs}}$ and $1 \le at, bs \le ts$. Hence $at = bs$, and from $\gcd(t, s) = 1$, we deduce that $a = s$ and $b = t$. Thus $\beta = \gamma$, and since $|\Delta \cap \mathrm{Supp}(c)| = t$, Part (iv) follows. Hence Parts (v) and (vi) follow from (4.1). □

The following shows that if $H = \langle x, y \rangle$ with $x \notin M$ and $y \in M$, then there are restrictions on $\mathcal{H}$. Recall that for $y = c_1 c_2 \cdots c_t \in \mathrm{S}_n$ written as a product of disjoint cycles, we let $\Theta_i = \mathrm{Supp}(c_i)$ for $1 \le i \le t$.

Lemma 4.2.14. *Let* $k, m \ge 2$*, let* $n = mk$*, let* $G = \mathrm{S}_n$ *or* A_n*, let* $M = (\mathrm{S}_k \mathrm{wr} \mathrm{S}_m) \cap G$ *with unique non-trivial* $\mathcal{M} = \{\Omega_1, \ldots, \Omega_m\}$*, let* $x \in G \backslash M$ *and let* $y \in M$ *with disjoint cycle decomposition* $c_1 \ldots c_t$*. If* $H = \langle x, y \rangle$ *is transitive and imprimitive with non-trivial block system* $\mathcal{H}$*, then for* $1 \le i, j \le t$ *the following hold.*

(i) *If* $\Theta_i \cap \Theta_i^x \ne \emptyset$*, then* $l(c_i^{\mathcal{H}}) \ne 1$*. In particular if* $l(c_i) > \frac{n}{2}$*, then* $l(c_i^{\mathcal{H}}) \ne 1$*.*

(ii) *If* $l(c_i)$ *does not divide* $l(c_j)$ *for all* $j \ne i$*, then* $l(c_i^{\mathcal{H}}) \ne l(c_i)$*.*

(iii) *Let* $\alpha \in \Theta_i$ *and* $\alpha^x \in \Theta_j$*. If there exist* $\Delta \in \mathcal{H}$ *such that* $\Delta, \Delta^x \in \mathrm{Supp}(c_i^{\mathcal{H}})$ *and* $\alpha \in \Delta$*, then* $l(c_i^{\mathcal{H}})$ *divides* $l(c_j)$*.*

(iv) *If there exists* $\{r_1, \ldots, r_s\} \subsetneq \{1, \ldots, m\}$ *such that* $\Omega_{r_1} \cup \cdots \cup \Omega_{r_s} = \mathrm{Supp}(c_i)$*, then* $\mathcal{M} \backslash \{\Omega_{r_1}, \cdots, \Omega_{r_s}\} \not\subseteq \mathcal{H}$*.*

(v) *If there exist $1 \leq i, j \leq t$ and $\Delta \in \mathcal{H}$ such that $l(c_i) > l(c_j)$ and $\Delta \subseteq \Theta_i \cup \Theta_j$, then $|\Delta \cap \Theta_i| \neq 1$. In particular, if $|\Delta| = 2$, then either $\Delta \subseteq \Theta_i$ or $\Delta \subseteq \Theta_j$.*

Proof. (i) If $l(c_i^{\mathcal{H}}) = 1$ then there exists $\Delta \in \mathcal{H}$ with $\Theta_i \subseteq \Delta$. Hence $\Delta^y = \Delta$. If $\Theta_i^x \cap \Theta_i \neq \emptyset$, then $\Delta^x = \Delta$, and so $\Delta^{\langle x,y \rangle} = \Delta$. Since $H = \langle x, y \rangle$ is transitive, it follows that $\Delta = \Omega$, a contradiction.

(ii) Suppose, by way of a contradiction, that $l(c_i^{\mathcal{H}}) = l(c_i)$ and let $\Delta \in \mathrm{Supp}(c_i^{\mathcal{H}})$. Then $|\Delta \cap \Theta_i| = 1$ and $|\Theta_i| > 1$. Since $\mathcal{H}$ is non-trivial, it follows that there exists $\alpha \in \Delta \backslash \Theta_i$. If $\alpha \notin \mathrm{Supp}(y)$ then $\alpha^y = \alpha$ and so $\Delta^y = \Delta$. Hence $\Theta_i \subseteq \Delta$, a contradiction since $|\Delta \cap \Theta_i| = 1$ and $|\Theta_i| > 1$. Therefore $\alpha \in \Theta_j$ for some $j \neq i$, and so $\Delta \in \mathrm{Supp}(c_j^{\mathcal{H}})$. Hence $c_j^{\mathcal{H}} = c_i^{\mathcal{H}}$ by Lemma 4.2.11(i), and in particular $l(c_j^{\mathcal{H}}) = l(c_i^{\mathcal{H}}) = l(c_i)$. Therefore $l(c_i)$ divides $l(c_j)$ by Lemma 4.2.10, a contradiction.

(iii) From $\alpha \in \Delta$, we deduce that $\alpha^x \in \Delta^x$. Therefore $\alpha^x \in \Delta^x \cap \Theta_j$, and so $\Delta^x \in \mathrm{Supp}(c_i^{\mathcal{H}}) \cap \mathrm{Supp}(c_j^{\mathcal{H}})$. Hence $c_i^{\mathcal{H}} = c_j^{\mathcal{H}}$ by Lemma 4.2.11(i), and so in particular $l(c_i^{\mathcal{H}}) = l(c_j^{\mathcal{H}})$. Therefore $l(c_i^{\mathcal{H}}) \mid l(c_j)$ by Lemma 4.2.10.

(iv) Suppose that $\mathcal{M} \backslash \{\Omega_{r_1}, \ldots, \Omega_{r_s}\} \subseteq \mathcal{H}$. Then the H-block size is k, and so $|\mathcal{H}| = m$. Let $\Delta_1, \ldots, \Delta_s$ be the remaining H-blocks. Then

$$\Omega_{r_1} \cup \cdots \cup \Omega_{r_s} = \mathrm{Supp}(c_i) = \Delta_1 \cup \cdots \cup \Delta_s \quad \text{and so} \quad l(c_i^{\mathcal{H}}) = s = l(c_i^{\mathcal{M}}).$$

Hence exists $1 \leq j \leq s$ and $\gamma \in \Omega$ such that $\gamma \in \Omega_{r_1} \cap \Delta_j$. Therefore by Lemma 4.2.13(i)

$$\Delta_j = \Delta_j \cap \mathrm{Supp}(c_i) = \Omega_{r_1} \cap \mathrm{Supp}(c_i) = \Omega_{r_1}.$$

By taking translates of Δ_j under y it follows that $\{\Delta_1, \ldots, \Delta_s\} = \{\Omega_{r_1}, \ldots, \Omega_{r_s}\}$, and so $\mathcal{H} = \mathcal{M}$. A contradiction since $x \in H \backslash M$.

(v) If $|\Delta \cap \Theta_i| = 0$ then the result holds. Hence assume that $|\Delta \cap \Theta_i| \geq 1$. If $\Delta \subseteq \Theta_i$, then the result holds since $\mathcal{H}$ is non-trivial. If $\Delta \not\subseteq \Theta_i$, then there exist $\alpha \in \Delta \cap \Theta_i$ and $\beta \in \Delta \cap \Theta_j$. Since $\beta^{y^{l(c_j)}} = \beta$ it follows that $\Delta^{y^{l(c_j)}} = \Delta$ and so $\alpha^{y^{l(c_j)}} \in \Delta$. Now $l(c_i) > l(c_j)$ implies that $\alpha^{y^{l(c_j)}} \neq \alpha$, and the result follows. □

We now give some conditions on cycle type and support which are sufficient to show that a group is primitive.

Lemma 4.2.15. *Let $x, y \in \mathrm{S}_n$, let $y = c_1 c_2 \cdots c_t$ be the disjoint cycle decomposition of y, and let $|\Theta_1| = q_1 q_2$ for distinct primes q_1 and q_2. Then $H = \langle x, y \rangle$ is primitive if all the following hold.*

(i) *There exist $2 \leq i, j \leq t$ (not necessarily distinct) such that $q_1 \nmid |\Theta_i|$ and $q_2 \nmid |\Theta_j|$, and $q_1 q_2 \nmid |\Theta_l|$ for $2 \leq l \leq t$.*

(ii) *There exist $\upsilon, \phi \in \Theta_1$ such that $\upsilon^x \in \Theta_i$ and $\phi^x \in \Theta_j$.*

(iii) *One of the following holds.*

(a) *There exist $\psi, \omega \in \Theta_1$ (not necessarily distinct) such that $\psi \in \upsilon^{\langle y^{q_1}\rangle}$, $\omega \in \phi^{\langle y^{q_2}\rangle}$ and $\{\psi, \omega\}^x \subseteq \Theta_1$.*

(b) *For υ and ϕ as in (ii), $\upsilon^y = \phi$ and $\upsilon^{\langle y^{q_1}\rangle} \subseteq \{\upsilon\} \cup \mathrm{Fix}(x)$.*

Proof. We begin by showing that Parts (i), (ii) and (iii)(b) implies Part (iii)(a). Let $\psi \in \upsilon^{\langle y^{q_1}\rangle}\backslash\{\upsilon\} \subseteq \mathrm{Fix}(x)$ so that $\psi = \psi^x \in \Theta_1$ and $\psi \in \upsilon^{y^{\langle q_1\rangle}}$. Since $\gcd(q_1, q_2) = 1$ there exists $a_1, a_2 \in \mathbb{Z}$ such that $a_1q_1 + a_2q_2 = 1$ and $q_2 \nmid a_1$. Hence

$$\omega := \upsilon^{y^{a_1q_1}} = \upsilon^{y^{1-a_2q_2}} = \phi^{y^{-a_2q_2}} \in \phi^{\langle y^{q_2}\rangle}.$$

Since $q_2 \nmid a_1$ it follows that $\upsilon^{y^{a_1q_1}} \neq \upsilon$, and so $\omega \in \upsilon^{\langle y^{q_1}\rangle}\backslash\{\upsilon\} \subseteq \mathrm{Fix}(x)$. Therefore $\omega, \omega^x \in \Theta_1$ and so Part (iii)(a) holds.

We now show that if Parts (i), (ii) and (iii)(a) hold, then H is primitive. Assume, by way of a contradiction, that H has a non-trivial block system $\mathcal{H}$. We proceed by considering the possibilities for $l(c_1^{\mathcal{H}})$. By Part (i) and Lemma 4.2.14(ii), it follows that $l(c_1^{\mathcal{H}}) \neq q_1q_2$. Since $\psi, \psi^x \in \Theta_1$ by Part (iii)(a), Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$.

If $l(c_1^{\mathcal{H}}) = q_1$, then by Part (iii)(a) there exists $\Delta \in \mathrm{Supp}(c_1^{\mathcal{H}})$ which contains υ and ψ, and so $\upsilon^x, \psi^x \in \Delta^x$. Since $\psi^x \in \Theta_1$ it follows that $\Delta^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$. Hence from $\upsilon^x \in \Theta_i$ and $q_1 \nmid |\Theta_i|$ we reach a contradiction by Lemma 4.2.14(iii).

If $l(c_1^{\mathcal{H}}) = q_2$, then by Part (iii)(a) there exists $\Delta \in \mathrm{Supp}(c_1^{\mathcal{H}})$ which contains $\omega, \phi \in \Delta$, and so $\omega^x, \phi^x \in \Delta^x$. Since $\omega^x \in \Theta_1$ it follows that $\Delta^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$. Since $\phi^x \in \Theta_j$ and $q_2 \nmid |\Theta_j|$ we reach a contradiction by Lemma 4.2.14(iii). Hence $l(c_1^{\mathcal{H}}) \neq 1, q_1, q_2, q_1q_2$, giving a contradiction by Lemma 4.2.10. □

4.3 Jordan elements

Let G be a primitive subgroup of S_n. In 1873 Jordan [32] proved that if G contains a cycle of prime order fixing at least 3 points, then G is either A_n or S_n. Jordan also made the following claim, that was later proved by Manning [46]. Let $q < 6$, and let $p > q$ be a prime. If $n > pq + q + 1$ and $G \leq \mathrm{S}_n$ is primitive and contains an element of order p and support size pq, then $\mathrm{A}_n \leq G$.

More recently Jones [31] showed, using the classification of finite simple groups, that if $n \geq 12$ and $G \leq \mathrm{S}_n$ is primitive and contains a cycle fixing at least 3 points, then $\mathrm{A}_n \leq G$.

In this section we introduce other sufficient conditions for a primitive subgroup of S_n to contain A_n.

Definition 4.3.1. An element $g \in \mathrm{S}_n$ is a *Jordan element* if all primitive subgroups of S_n which contain g also contain A_n.

Definition 4.3.2. Let $g \in \mathrm{S}_n$ be an element of prime order p and support size pq. We call g a *Wielandt element* if

$$\begin{array}{rccccccccc} q = & 1 & 2 & 3 & 4 & 4 & 5 & 6 & 7 & \geq 8, \\ p \geq & 2 & 5 & 5 & 7 & 5 & 7 & 11 & 11 & 2q-1, \\ n - pq > & 2 & 2 & 3 & 4 & 5 & 6 & 6 & 8 & 4q-4. \end{array}$$

In particular, by the final column, if $q \geq 8$, $p \geq 2q-1$ and $n > (p+4)q-4$, then an element of S_n with order p and support size pq is a Wielandt element.

We now give some examples of Jordan elements.

Definition 4.3.3. Let $n \geq 12$. Define the following subsets of $\mathrm{S}_n \backslash \{1\}$.

(i) $\mathcal{J}_t$ is the set of elements which are a product of two transpositions.

(ii) $\mathcal{J}_c$ is the set of cycles which fix at least three points.

(iii) $\mathcal{J}_s$ is the set of elements with support size at most $2(\sqrt{n}-1)$.

(iv) $\mathcal{J}_w$ is the set of Wielandt elements.

Theorem 4.3.4. *Let $n \geq 12$, let $\mathcal{J}_t, \mathcal{J}_c, \mathcal{J}_s, \mathcal{J}_w$ be as in Definition 4.3.3 and let $\mathcal{J} = \mathcal{J}_t \cup \mathcal{J}_c \cup \mathcal{J}_s \cup \mathcal{J}_w$. If $x \in \mathrm{S}_n$ and there exists $t \in \mathbb{N}$ for which $x^t \in \mathcal{J}$, then x is a Jordan element.*

Proof. If H is a group containing x, then H contains x^t for all $t \in \mathbb{N}$. Hence if x^t is a Jordan element then x is also. Therefore if all elements in $\mathcal{J}$ are Jordan elements then the result follows. For $\mathcal{J}_t, \mathcal{J}_c, \mathcal{J}_s$ and $\mathcal{J}_w$ see [58, p43], [31, Corollary 1.3], [40, Corollary 3] and [58, Theorem 13.10] respectively. □

The following is immediate.

Lemma 4.3.5. *Let $n \geq 12$ and let $x \in \mathcal{J}$. Then $\mathrm{Fix}(x) \neq \emptyset$.*

The next theorem is another result of Jones from [31] which we use to prove a result similar to Jordan elements.

Theorem 4.3.6. *[31, 1.3] Let $G \leq \mathrm{S}_n$ be a primitive permutation group which does not contain A_n. If G contains an n-cycle then one of the following holds.*

(i) *$C_p \leq G \leq \mathrm{AGL}_1(p)$ with $n = p$;*

(ii) $\mathrm{PGL}_d(q) \leq G \leq \mathrm{P\Gamma L}_d(q)$ *with* $n = \frac{(q^d-1)}{(q-1)}$ *and* $d \geq 2$ *for some prime power* q*; or*

(iii) $G = L_2(11), \mathrm{M}_{11}, \mathrm{M}_{23}$ *with* $n = 11, 11$ *or* 23 *respectively.*

Using the above we prove the following.

Theorem 4.3.7. *Let* $\Omega = \{1, \ldots, n\}$*, let* $\mathrm{S}_n = \mathrm{Sym}(\{1, \ldots, n\})$*, let* $x \in \mathrm{S}_n \backslash \{1\}$ *such that* $|\mathrm{Supp}(x)| < \frac{n}{2}$*, and let* $y \in \mathrm{S}_n$ *be an* n*-cycle. If* $H \leq \mathrm{S}_n$ *is primitive and* $x, y \in H$*, then* $\mathrm{A}_n \leq H$*.*

Proof. By Theorem [31, 1.3] each primitive subgroup of S_n containing an n-cycle either contains A_n, or is as in Theorem 4.3.6(i)-(iii). As we shall see in Lemma 4.6.8(ii), non-identity elements of $\mathrm{AGL}_1(p)$ fix at most one point. Proposition [29, 3.1(ii)] shows that a non-identity element of $\mathrm{P\Gamma L}_d(q)$ fixes at most $\frac{n}{2}$ points of Ω. If $(G, n) = (L_{11}, 11), (\mathrm{M}_{11}, 11)$ or $(\mathrm{M}_{23}, 23)$, then a quick calculation in Magma shows that non-identity elements of G fix at most 3, 3 or 7 points respectively. Hence from $x \in H$ the result follows. □

4.4 Number theory

In Chapters 5 and 6 we generate subgroups H of S_n which are primitive and contain Jordan elements, so H is either A_n or S_n. To prove primitivity we use the results in Section 4.2, many of which rely on H containing elements whose disjoint cycle decomposition contains a prime cycle or cycle with length coprime to the other cycles. To prove the existence of a Jordan element we need to show that H contains an element of "small" support size, a single cycle, or a product of prime cycles satisfying certain properties.

In this section we prove the existence of primes within various integer ranges satisfying specific conditions.

For some small cases we quote results from Chapter 8 - in which we verify the result computationally or directly. Throughout this subsection, ln is the natural logarithm. Unless otherwise referenced the following results do not appear to be in the literature. We begin with Bertrand's Postulate.

Theorem 4.4.1 (Bertrand's Postulate. See for example [17, §1])**.** *Let* $j, k \in \mathbb{N}$*. If* $j \geq 4$*, then there exists at least one prime* p *such that* $j < p < 2j - 2$*. Thus if* $k \geq 7$*, then there exists a prime* p_k *with* $\frac{k}{2} < p_k < k - 1$*.*

Notation 4.4.2. Let $k \in \mathbb{N}$ with $k \geq 7$. We use p_k to denote any prime in the range $(\frac{k}{2}, k-1)$, and call such any such prime a *Bertrand prime.*

For example if $k = 13$ then 7 and 11 are both Bertrand primes and p_k could denote either 7 or 11.

We now prove an elementary lemma relating $n-k$ to p_k.

Lemma 4.4.3. *Let $n > k > \frac{n}{2} \geq 3$ and let p_k be a Bertrand prime. If $p_k \mid (n-k)$ then $p_k = n-k$, and if $p_k \mid (n-k-1)$ then $p_k = n-k-1$.*

Proof. From $\frac{n}{2} < k$ and $\frac{k}{2} < p_k$ we deduce that $n-k-1 < n-k < k < 2p_k$. Hence the result follows. □

For $x \in \mathbb{N}$, the *prime-counting function* $\pi(x)$ is the number of primes less than or equal to x. Using this function Theorem 4.4.1 can be rephrased as $\pi(k-2) - \pi(\frac{k}{2}) \geq 1$.

Theorem 4.4.4 ([49, Corollary 1 & 3]). *Let $x \in \mathbb{N}$ and let $\pi(x)$ be as above.*

(i) *If $x \geq 17$, then $\pi(x) > \frac{x}{\ln(x)}$.*

(ii) *If $x \geq 21$, then $\frac{3x}{5\ln(x)} < \pi(2x) - \pi(x)$.*

We now prove some technical results using Theorems 4.4.1 and 4.4.4 which ensure the existence of useful primes. The following two lemmas will be used only in Chapter 5.

Lemma 4.4.5. *Let $n > k > \frac{n}{2}$ and $k \geq 10$. Then there exists an odd prime $p^{(1)} \leq k-5$ such that $p^{(1)} \nmid (n-k)$.*

Proof. Let $Q = \{2 \leq q \leq k-5 \ : \ q \text{ prime } \}$. The product of the set of prime divisors of $n-k$ is at most $n-k$. Hence if

$$2(n-k) < \prod_{q \in Q} q, \tag{4.2}$$

then $(n-k) < \prod_{q \in Q \setminus \{2\}} q$, and so there exists $q \in Q \setminus \{2\}$ such that $q \nmid (n-k)$. Therefore the result holds with $p^{(1)} = q$. Hence we show that (4.2) holds.

First assume that $10 \leq k \leq 15$. Then $\{2,3,5\} \subseteq Q$ and so

$$2(n-k) \leq 2(k-1) \leq 2 \cdot 14 < 30 = 2 \cdot 3 \cdot 5 \leq \prod_{q \in Q} q.$$

Hence (4.2) holds.

Assume that $k > 15$, and let $m := k-5 > 10$. Hence by Theorem 4.4.1 there exists a prime p_m satisfying $5 < \frac{m}{2} < p_m < m-1$. Hence $2, 3, 5$ and p_m are distinct elements in Q. From $\frac{n}{2} < k$, it follows that $n < 2k$, and so $n-k \leq k-1 = m+4$. Clearly $8 < 13m$, and so $2(m+4) < 15m$. Hence

$$2(n-k) \leq 2(m+4) < 15m < 3 \cdot 5 \cdot (2p_m) \leq \prod_{q \in Q} q,$$

as required. □

Lemma 4.4.6. *Let $n > k > \frac{n}{2}$ and $n-k > 10$. Then either*

(i) *there exists a prime $p^{(2)}$ such that $2 < p^{(2)} < n-k-3$ and $p^{(2)} \nmid k$; or*

(ii) $n-k+1 < 2(\sqrt{n}-1)$.

Proof. First let $10 < n-k < 26$ and let $P = \{2 < q < n-k-3 \mid q \text{ prime}\}$. If Part (i) does not hold, then all primes $q \in P$ divide k, and so $\prod_{q \in P} q \leq k < n$. For each $n-k$ satisfying $10 < n-k < 26$ it can be checked via [33, Code 18] in Magma that

$$\frac{(n-k+3)^2}{4} < \prod_{q \in P} q.$$

Hence if (i) does not hold then $(n-k+3)^2/4 < n$ and so $n-k+3 < \sqrt{4n}$. Therefore $n-k+1 < 2(\sqrt{n}-1)$, satisfying Part (ii).

Now let $n-k \geq 26$, and let $m = n-k-3$, so that $m \geq 23$. We first prove that

$$2\Big(\pi(m-1)-4\Big) > \ln\left(2\Big(\frac{m}{2}+3\Big)^2\right). \tag{4.3}$$

To do so let $y := y(m)$ be the following function of m

$$y = (m-1) - \ln\Big(\frac{m}{2}+3\Big)\ln(m-1) - \frac{1}{2}\Big(\ln(2)+8\Big)\ln(m-1).$$

Then

$$\begin{aligned}\frac{dy}{dm} &= 1 - \frac{\ln\left(\frac{m}{2}+3\right)}{m-1} - \frac{\ln(m-1)}{\frac{m}{2}+3}\cdot\frac{1}{2} - \frac{\frac{1}{2}(\ln(2)+8)}{m-1} \\ &= 1 - \frac{\ln\left(\frac{m}{2}+3\right)}{m-1} - \frac{\ln(m-1)}{m+6} - \frac{\ln(2)+8}{2(m-1)}.\end{aligned}$$

The functions $\frac{\ln(\frac{m}{2}+3)}{m-1}$ and $\frac{\ln(2)+8}{2(m-1)}$ are monotonically decreasing for $m \geq 2$, the function $\frac{\ln(m-1)}{m+6}$ is monotonically decreasing for $m \geq 9$. Hence $\frac{dy}{dm}$ is monotonically increasing for $m \geq 9$. Since $\frac{dy}{dm}$ is positive at $m = 9$, it follows that $\frac{dy}{dm}$ is positive for $m \geq 9$. From $y(23) > 0$, we deduce that y is positive for $m \geq 23$. Thus for $m \geq 23$

$$(m-1) - 4\ln(m-1) > \ln\Big(\frac{m}{2}+3\Big)\ln(m-1) + \frac{1}{2}\ln(2)\ln(m-1),$$

and so

$$2\Big(\frac{m-1}{\ln(m-1)} - 4\Big) > 2\ln\Big(\frac{m}{2}+3\Big) + \ln(2) = \ln\left(2\Big(\frac{m}{2}+3\Big)^2\right). \tag{4.4}$$

By Theorem 4.4.4(i), $\pi(m-1) > \frac{m-1}{\ln(m-1)}$, and so (4.4) implies (4.3).

Let $Q = \{2 \leq q < m \mid q \text{ prime}\}$ and $Q_0 = \{q \in Q : q > 7\}$. Then $Q_0 = Q \backslash \{2, 3, 5, 7\}$, and so $|Q_0| = \pi(m-1) - 4$. We use (4.3) to show that either there exists $q \in Q$ satisfying (i), or that (ii) holds. Observe that if $q \in Q_0$, then $\ln(q) > 2$. Then by (4.3),

$$\ln\left(\prod_{q \in Q} q\right) = \sum_{q \in Q} \ln(q) > \sum_{q \in Q_0} \ln(q) > \sum_{q \in Q_0} 2 = 2\Big(\pi(m-1) - 4\Big) > \ln\left(2\Big(\frac{m}{2} + 3\Big)^2\right).$$

Thus

$$\prod_{q \in Q} q > 2\Big(\frac{m}{2} + 3\Big)^2.$$

If (i) does not hold, then $q \mid k$ for all odd primes $q \in Q$. Hence k is greater than or equal to the product of all such primes, so

$$2n > 2k \geq \prod_{q \in Q} q > 2\Big(\frac{m}{2} + 3\Big)^2.$$

Hence $\sqrt{n} > \frac{m}{2} + 3$ and so

$$2(\sqrt{n} - 1) > m + 4 = (n - k - 3) + 4 = n - k + 1,$$

which gives Part (ii). Hence the lemma holds. □

The remainder of the results in this section are only used in Chapter 6. Let $m, k \geq 2$ and $n = mk$. Recall that p_k denotes any prime which satisfies $\frac{k}{2} < p_k < k - 1$, similarly let p_m denotes any prime satisfying $\frac{m}{2} < p_m < m - 1$. Let $\mathcal{J}_w$ is the set of elements of S_n satisfying Definition 4.3.2.

Lemma 4.4.7. *Let $k \geq 26$. Then there exists p_k such that $p_k \geq 23$.*

Proof. If $26 \leq k \leq 37$, then $\frac{k}{2} \leq 18.5 < p_k < 25 \leq k - 1$, and so we may let $p_k = 23$. If $k \geq 38$, then $\frac{k}{2} \geq 19$. Hence $p_k > 19$, and so $p_k \geq 23$. □

Lemma 4.4.8. *Let $23 \leq k \leq m < 4k - 2$. Then there exists a prime q such that $q \nmid m$, and for all possible p_k every element in S_n with cycle type $1^{n - p_k q} \cdot {p_k}^q$ is in $\mathcal{J}_w$.*

Proof. First assume that $k \leq 66$ and $m \neq 210$. If $x \in \mathbb{N}$ is divisible by $2, 3, 5$ and 7, then either $x = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, or $x \geq 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$. Thus from $m < 4k - 2 \leq 262$ and $m \neq 210$, it follows that there exists $q \in \{2, 3, 5, 7\}$ such that $q \nmid m$. From $p_k > \frac{k}{2} > 11$ it follows that

$$n = mk \geq k^2 > kp_k = (k-1)p_k + p_k > qp_k + 11.$$

Hence for $q = 2, 3, 5$ and 7 the result follows by consulting the third, fourth, seventh and ninth respective columns of Definition 4.3.2.

Let $m = 210$, let $k \leq 66$ and let $q = 11$. Then $q \nmid m$. By assumption $m < 4k - 2$, and so $54 \leq k \leq 66$. Therefore $p_k > \frac{k}{2} \geq 27 > 2q - 1$ and

$$n = 210k = 11k + 199k > qp_k + 4q,$$

and so the final column of Definition 4.3.2 is satisfied.

Hence we may assume that $k \geq 67$. We first show if q is prime and $11 \leq q \leq \frac{k+2}{4}$, then an element of S_n with cycle type $1^{n-p_kq} \cdot p_k{}^q$ is in $\mathcal{J}_w$. In particular, we verify the three conditions in the final column on Definition 4.3.2 - $p_k \geq 2q - 1$ and $n > (p_k + 4)q - 4$. From $q \leq \frac{k+2}{4}$ it follows that $4q - 2 \leq k < 2p_k$, hence $p_k > 2q - 1$ and the first condition is satisfied. We now show that $n > (p_k + 4)q - 4$. Since $3k^2 - 5k + 10$ is a positive quadratic with no real roots it follows that $3k^2 - 5k + 10 > 0$, and so $4k^2 > k^2 + 5k - 10$. Therefore

$$\begin{aligned} k^2 &> \frac{k^2 + 5k + 6 - 16}{4} \\ &= \frac{(k^2 + k - 2) + (4k + 8)}{4} - 4 \\ &= \frac{(k - 1)(k + 2) + 4(k + 2)}{4} - 4. \end{aligned}$$

Hence since $n = mk \geq k^2$, it follows that

$$n > (k - 1)\frac{(k + 2)}{4} + 4\frac{(k + 2)}{4} - 4. \tag{4.5}$$

By assumption $q \leq \frac{k+2}{4}$, and by Theorem 4.4.1, $p_k \leq k - 1$. Hence (4.5) implies that

$$n > p_kq + 4q - 4.$$

Thus if there exists a prime q such that $11 \leq q \leq \frac{k+2}{4}$ and $q \nmid m$, then the result holds. We now show the existence of such a prime.

First let $66 \leq k \leq 105$. Then if $q \in \{11, 13, 17\}$ it follows that

$$11 \leq q \leq 17 = \frac{66 + 2}{8} \leq \frac{k + 2}{4} \quad \text{and} \quad m < 4k - 2 \leq 4(105) - 2 = 418 < 11 \cdot 13 \cdot 17.$$

Hence there exists $q \in \{11, 13, 17\}$ such that $8 \leq q \leq \frac{k+2}{4}$ and $q \nmid m$. Therefore the result holds for $k \leq 105$.

Now let $k \geq 106$ and let $t = \lfloor \frac{k+2}{4} \rfloor$. Then

$$13.5 = \frac{1}{2}\left\lfloor \frac{106+2}{4} \right\rfloor \leq \frac{1}{2}\left\lfloor \frac{k+2}{4} \right\rfloor = \frac{t}{2} < p_t < t-1 < \frac{k+2}{4}.$$

Therefore $11, 13$ and p_t are distinct increasing primes bounded above by $\frac{k+2}{4}$. In addition,

$$m < 4k - 2 < 11 \cdot 13 \cdot \frac{1}{2}\left\lfloor \frac{k+2}{4} \right\rfloor < 11 \cdot 13 \cdot p_t.$$

and so there exists $q \in \{11, 13, p_t\}$ such that $q \nmid m$. Hence the result follows. □

Lemma 4.4.9. *Let $m \geq 19$. Then there exists a prime q such that $q < \frac{m}{4}$ and $q \nmid m$.*

Proof. For $19 \leq m \leq 43$ it follows by [33, Code 13] in Magma that there exists $q \in \{2, 3, 5, 7\}$ as required. Hence we may assume that $m \geq 44$. Let $t = \lfloor \frac{m}{4} \rfloor$, so that $\frac{m-3}{4} \leq t \leq \frac{m}{4}$. Then $t > 10$, and so by Theorem 4.4.1 there exists a prime p_t such that

$$5 < \frac{t}{2} < p_t < t - 1 < \frac{m}{4}.$$

Hence 2, 3, 5 and p_t are distinct and less than $\frac{m}{4}$. Since $\frac{m-3}{4} \leq t$, it follows that $m \leq 4t + 3 < 15t$, and so

$$m < 15t < 3 \cdot 5 \cdot 2p_t.$$

Therefore there exists $q \in \{2, 3, 5, p_t\}$ satisfying the lemma. □

We now use Theorem 4.4.4(ii) to find a lower bound on the number of Bertrand primes as in Theorem 4.4.1.

Proposition 4.4.10. *For $19 \leq k \leq 39$ let $t = 3$, for $40 \leq k \leq 72$ let $t = 4$, and for $k \geq 73$ and let*

$$t = \left\lfloor \frac{3k}{10 \ln(\frac{k+1}{2})} - 2 \right\rfloor.$$

Then there exist primes ${p_k}^{(1)}, {p_k}^{(2)}, \ldots, {p_k}^{(t)}$ such that

$$\frac{k}{2} < {p_k}^{(1)} \leq {p_k}^{(2)} - 2 \leq {p_k}^{(3)} - 4 \leq \cdots \leq {p_k}^{(t)} - 2(t-1) < k - 2(t-1) - 1.$$

Proof. We begin by verifying a few cases directly. Let $P = ({p_k}^{(1)}, \ldots, {p_k}^{(t)})$. If $19 \leq k \leq 21$, then let $P = (11, 13, 17)$; if $22 \leq k \leq 25$, then let $P = (13, 17, 19)$; if $26 \leq k \leq 33$, then let $P = (17, 19, 23)$; and if $34 \leq k \leq 39$, then let $P = (23, 29, 31)$. Hence the result holds for $19 \leq k \leq 39$. If $40 \leq k \leq 45$, then let $P = (23, 29, 31, 37)$; if $46 \leq k \leq 61$, then let $P = (31, 37, 41, 43)$; and if $61 \leq k \leq 72$, then let $P = (37, 41, 43, 47)$. Hence the result holds for $40 \leq k \leq 72$.

Now let $k \geq 73$. Let $x = \lceil \frac{k}{2} \rceil$, so that $\frac{k}{2} \leq x \leq \frac{k+1}{2}$. Let

$$Q = \{x+1 \leq q \leq 2x \ : \ q \text{ prime}\} \quad \text{and} \quad R = \Big\{q \text{ prime} : \frac{k}{2} < q \leq k+1\Big\},$$

so that $|Q| = \pi(2x) - \pi(x)$ and $Q \subseteq R$. Hence by Theorem 4.4.4(ii), the size of Q, and so the size of R also, is at least

$$\frac{3x}{5\ln(x)} \geq \frac{3\frac{k}{2}}{5\ln(\frac{k+1}{2})} = \frac{3k}{10\ln(\frac{k+1}{2})}.$$

Therefore $|R| \geq t+2$. If $q \in R\backslash\{k-1, k, k+1\}$, then $\frac{k}{2} < q < k-1$. Since $\frac{k}{2} > 20$, every element of R is odd. Hence R contains at most two of $\{k-1, k, k+1\}$ thus $|R\backslash\{k-1, k, k+1\}| \geq |R| - 2 \geq t$. Hence $R\backslash\{k-1, k, k+1\}$ contains distinct increasing primes ${p_k}^{(1)}, {p_k}^{(2)}, {p_k}^{(3)}, \ldots, {p_k}^{(t)}$. Then in particular, $\frac{k}{2} < {p_k}^{(1)}$ and ${p_k}^{(t)} < k-1$. Therefore since all elements of R are odd it follows that

$$\frac{k}{2} < {p_k}^{(1)} \leq {p_k}^{(2)} - 2 \leq {p_k}^{(3)} - 4 \leq \cdots \leq {p_k}^{(t)} - 2(t-1) < k - 2(t-1) - 1.$$

□

For the remainder of this section we use Proposition 4.4.10 to show the existence of primes with certain properties.

Lemma 4.4.11. *Let $k \geq 26$, let $m \geq 19$ and let $n = mk$. Then at least one of the following holds.*

(i) *There exists a prime p_k such that $\frac{k}{2} < p_k < k-1$ and $p_k \nmid (m-1)$.*

(ii) *There exist primes q and p_k such that $p_k < q$, $q \nmid mk$, $kq < 2(\sqrt{n} - 1)$ and $k < (m-q)$.*

Proof. First let $26 \leq k \leq 39$. Then the result follows by [33, Code 14], which we summarise here. Let $W = \big\{\frac{k}{2} < w < k-1 \ : \ w \text{ prime}\big\}$. Then it can be directly verified that $|W| \geq 2$ for each k. Suppose that (i) does not hold. Then each $w \in W$ divides $m-1$, and so

$$r := \prod_{w \in W} w \leq m - 1 < m. \tag{4.6}$$

Let $p_k := \min(W)$ and $q := \min(W\backslash\{p_k\})$, then $p_k < q$ automatically. Since $q \mid (m-1)$ and $\frac{k}{2} < q < k-1$ it follows that $q \nmid mk$. For each $26 \leq k \leq 39$, we find that $k < (r-q)$ and $kq < 2\big(\sqrt{kr} - 1\big)$. Hence p_k and q satisfy (ii) by (4.6).

Now let $k \geq 40$ and let ${p_k}^{(1)}, {p_k}^{(2)}, {p_k}^{(3)}, {p_k}^{(4)}$ be as in Proposition 4.4.10. Assume that

(i) does not hold. Then ${p_k}^{(i)} \mid (m-1)$ for $i = 1, 2, 3, 4$. Hence

$$\left(\frac{k}{2}\right)^4 < {p_k}^{(1)} \cdot {p_k}^{(2)} \cdot {p_k}^{(3)} \cdot {p_k}^{(4)} \leq m - 1 < m. \tag{4.7}$$

We show that $p_k := {p_k}^{(1)}$ and $q := {p_k}^{(2)}$ satisfy (ii). Clearly, $p_k < q$. Since $q \mid (m-1)$ and $\frac{k}{2} < q < k-1$ it follows that $q \nmid mk$. Since $k \geq 40$, it follows that $2k^2 + 4 < \sqrt{k}k^2$, and so $k^2 < \frac{k^2\sqrt{k}}{2} - 2$. Hence

$$kq < k^2 < \frac{k^2\sqrt{k}}{2} - 2 = 2\left(\sqrt{\left(\frac{k}{2}\right)^4}\sqrt{k} - 1\right).$$

Combining the above with (4.7) implies that $kq < 2(\sqrt{m}\sqrt{k} - 1) = 2(\sqrt{n} - 1)$. Since

$$k(k^2 - 16) \geq 40(40^2 - 16) > 16,$$

it follows that $\frac{1}{16}k(k^3 - 16k) > k$. Hence (4.7) and $q < k$ imply that

$$m - q > \left(\frac{k}{2}\right)^4 - k = \frac{1}{16}k(k^3 - 16k) > k. \quad \square$$

Lemma 4.4.12. *For $k \geq 19$ there exist primes p_k and ${p_k}'$ such that $\frac{k}{2} + 2 < p_k, {p_k}' < k - 1$.*

Proof. By Proposition 4.4.10 implies that there exist primes

$$\frac{k}{2} < {p_k}^{(1)} \leq {p_k}^{(2)} - 2 \leq {p_k}^{(3)} - 4 < k - 5.$$

Thus the lemma holds with $p_k := {p_k}^{(2)}$ and ${p_k}' := {p_k}^{(3)}$. □

Lemma 4.4.13. *If $k \geq 8$, then there exists a prime p_k such that $\frac{k}{2} < p_k < k - 2$.*

Proof. If $k = 8$ or 9, then let $p_k = 5$; if $10 \leq k \leq 13$, then let $p_k = 7$; if $14 \leq k \leq 18$ then let $p_k = 11$, and if $k \geq 19$ then by Proposition 4.4.10 there are at least 3 Bertrand primes, and so $p_k := {p_k}^{(1)} < k - 5$. □

Lemma 4.4.14. *Let either $k \geq 33$ and $m \geq 19$; or let $28 \leq k \leq 32$, $19 \leq m \leq 41$ and $m \neq 30$. There exists primes p_k and q such that $p_k, 2p_k \neq m - q$, $q < \frac{m}{4}$ and $q \nmid m$*

$$\frac{k+9}{2} \leq p_k \leq k - 4.$$

Proof. If $28 \leq k \leq 32$, $19 \leq m \leq 41$ and $m \neq 30$ then the holds holds by direct calculation in Magma using [33, Code 2].

Hence assume that $k \geq 33$ and $m \geq 19$. Therefore Lemma 4.4.9 holds, and so there exists a prime q with $q < \frac{m}{4}$ and $q \nmid m$. For $33 \leq k < 106$, using [33, Code 16] it can be checked directly that there exist at least 2 primes ${p_k}^{(1)}$ and ${p_k}^{(2)}$ in the range $\left[\frac{k+9}{2}, k-4\right]$. If $m-q$ is even, then $m-q \neq {p_k}^{(1)}, {p_k}^{(2)}$; and if $m-q$ is odd, then $m-q \neq 2{p_k}^{(1)}, 2{p_k}^{(2)}$. Hence at least one of ${p_k}^{(1)}$ and ${p_k}^{(2)}$ satisfies the lemma.

Now let $k \geq 106$. By Proposition 4.4.10 there exist primes

$$\frac{k}{2} < {p_k}^{(1)} \leq {p_k}^{(2)} - 2 \leq {p_k}^{(3)} - 4 \leq {p_k}^{(4)} - 6 \leq {p_k}^{(5)} - 8 < k - 9.$$

Therefore $\frac{k}{2} + 4 < {p_k}^{(3)}, {p_k}^{(4)} < k - 3$, and so $\frac{k+9}{2} \leq {p_k}^{(3)}, {p_k}^{(4)} \leq k - 4$. By considering the parity of $m - q$ as above, it follows that at least one of ${p_k}^{(3)}$ and ${p_k}^{(4)}$ satisfies the lemma. □

Lemma 4.4.15. *Let $m, k \geq 19$. Then there exist distinct primes p_k, ${p_k}'$ and p_m such that $p_m \leq m - 4$.*

Proof. By Proposition 4.4.10 there exist primes

$$\frac{m}{2} < p_m^{(1)} \leq p_m^{(2)} - 2 < m - 3 \quad \text{and} \quad \frac{k}{2} < {p_k}^{(1)} \leq {p_k}^{(2)} - 2 \leq {p_k}^{(3)} - 4 < k - 5.$$

Hence $p_m := p_m^{(1)} \leq m - 4$. At least two primes in $\{{p_k}^{(1)}, {p_k}^{(2)}, {p_k}^{(3)}\}$, which we denote p_k and ${p_k}'$, are not equal to p_m. □

Lemma 4.4.16. *Let $23 \leq k \leq m < 4k - 2$, let p_k and ${p_k}'$ be as in Lemma 4.4.15, and let q be as in Lemma 4.4.8, so that in particular $q \nmid m$. Then either p_k or ${p_k}'$ does not divide $(m - q)$.*

Proof. If $p_k, {p_k}' \mid (m-q)$, then $p_k{p_k}' \leq (m-q)$. Since $k \geq 23$, it follows that $k^2 > 16k-8$. Hence $\left(\frac{k}{2}\right)^2 > 4k - 2$, and so

$$4k - 2 < \left(\frac{k}{2}\right)^2 < p_k{p_k}' \leq m - q < m,$$

contradicting the assumption that $m < 4k - 2$. □

Lemma 4.4.17. *Let $m \geq 14$. Then there exists a prime p_m such that $\max\{10, \frac{m}{2}\} < p_m \leq m - 3$.*

Proof. If $m = 14$ or 15, then let $p_m = 11$; if $16 \leq m \leq 25$, then let $p_m = 13$; and if $26 \leq m \leq 42$, then let $p_m = 23$.

For $m > 42$, Proposition 4.4.10 implies that there exist primes

$$21 < \frac{m}{2} < p_m^{(1)} \leq p_m^{(2)} - 2 < m - 3.$$

Hence $p_m^{(1)}$ satisfies the lemma. □

Lemma 4.4.18. *Let $m, k \geq 18$. Then there exist distinct primes p_k and p_m satisfying $\frac{m+5}{2} \leq p_m \leq m - 5$ and $p_k \leq k - 5$; and if $k \leq m \leq 4k - 2$, then we may assume that $p_k \nmid (m - 2)$.*

Proof. We begin by introducing various primes. If $18 \leq m \leq 88$ and $18 \leq k \leq 88$, then by [33, Code 17] there exist distinct primes

$$p_k{}^{(a)} \leq k - 5 \text{ and } \frac{m+5}{2} \leq p_m^{(a)} \leq m - 5.$$

Let $l = m$ or k. If $l \geq 89$, then by Proposition 4.4.10 there exist primes

$$\frac{l}{2} < p_l^{(1)} \leq p_l^{(2)} - 2 \leq p_l^{(3)} - 4 \leq p_l^{(4)} - 6 \leq p_l^{(5)} - 8 < l - 9.$$

Hence $p_l^{(1)}, p_l^{(2)}, p_l^{(3)} \leq l - 5$ and $\frac{l+5}{2} \leq p_l^{(2)}, p_l^{(3)} \leq l - 5$.

First assume that $k \leq 88$. If $k \leq m \leq 4k - 2$ then the result holds by [33, Code 17], otherwise let $p_k = p_k{}^{(a)}$. If $m \leq 88$ then let $p_m := p_m^{(a)}$, and if $m \geq 89$ then let $p_m \in \{p_m^{(2)}, p_m^{(3)}\}$.

Next assume that $k \geq 89$. If $m \leq 88$ then let $p_m = p_m^{(a)}$, and if $m \geq 89$ then let $p_m := p_m^{(3)}$. We now show that one of $p_k{}^{(1)}$ and $p_k{}^{(2)}$ satisfies the lemma. If $k \leq m \leq 4k-2$ is not satisfied, either of $p_k{}^{(1)}$ and $p_k{}^{(2)}$ satisfy the lemma. Hence assume that $k \leq m \leq 4k - 2$. It is clear that $k^2 > 16k - 16$ and so $\left(\frac{k}{2}\right)^2 > 4k - 4$. Hence

$$m - 2 \leq 4k - 4 < \left(\frac{k}{2}\right)^2 < p_k{}^{(1)} \cdot p_k{}^{(2)},$$

and so at most one of $p_k{}^{(1)}$ and $p_k{}^{(2)}$ divides $m - 2$. Thus there exists $p_k \in \{p_k{}^{(1)}, p_k{}^{(2)}\}$ which satisfies the lemma. □

Lemma 4.4.19. *Let $18 \leq m < k$. Then there exist distinct primes p_m and p_k such that $p_k \neq m - 3$, $p_k \leq k - 6$ and $p_m \leq m - 6$.*

Proof. Let $l = m$ or k. If $l \geq 89$ then there exist primes

$$\frac{l}{2} < p_l^{(1)} \leq p_l^{(2)} - 2 \leq p_l^{(3)} - 4 \leq p_l^{(4)} - 6 \leq p_l^{(5)} - 8 < l - 9. \tag{4.8}$$

First let $18 \leq m < k \leq 89$. Then the result holds by [33, Code 18].

Now let $k \geq 89$ and $m \leq 88$. By [33, Code 18] there exists $p_m \leq m - 6$ and by (4.8) there exist $p_k^{(1)}, p_k^{(2)}, p_k^{(3)} \leq k - 6$. Hence we may let $p_k \in \{p_k^{(1)}, p_k^{(2)}, p_k^{(3)}\} \backslash \{p_m, m - 3\}$.

Finally if $k, m \geq 89$, then by (4.8) there exist $p_m^{(1)}, p_m^{(2)} \leq m - 6$ and ${p_k}^{(1)}, {p_k}^{(2)} \leq k - 6$. Therefore there exists $p_k \in \{{p_k}^{(1)}, {p_k}^{(2)}\} \backslash \{m-3\}$ and $p_m \in \{p_m^{(1)}, p_m^{(2)}\} \backslash \{p_k\}$, which satisfy the lemma. □

4.5 Generating graphs and cocliques

We begin by giving some history of the study of generation, generating graphs, cliques and cocliques - see Definitions 4.5.1 and 4.5.5.

A group G is *2-generated* if there exist $x, y \in G$ such that $\langle x, y \rangle = G$. In 1962 Steinberg [52] proved that all the finite simple groups known by 1962 were 2-generated. In addition, Steinberg speculated that it may be possible to insist that one generator has order 2 or that one generator is chosen to be an arbitrary non-identity element. This second property is called $\frac{3}{2}$*-generation*, and means that for all $x \in G \backslash \{1\}$ there exists $y \in G$ such that $\langle x, y \rangle = G$. In 2000 Guralnick and Kantor [29] proved that all finite simple groups are $\frac{3}{2}$-generated. Guralnick and Kantor also showed the following stronger result - for all finite simple groups G, there exists a conjugacy class C such that for all $x \in G \backslash \{1\}$ there exists $y \in C$ such that $G = \langle x, y \rangle$. More recently, Burness and Harper [9, 10] investigated the size of the smallest set $S \subseteq C$ such that for all $x \in G \backslash \{1\}$ there exists $y \in S$ such that $G = \langle x, y \rangle$. Such a set S is called a *uniform dominating set.*

One way to view such generation problems is via the generating graph. This enables the use of graph theoretic results to gain a deeper understanding of generation. See for example [42], in which Liebeck and Shalev first defined generating graphs and also used Turán's Theorem [56]. The authors prove that there exists a constant $c > 0$ such that for every finite simple group G, the generating graph $\Gamma(G)$ contains a clique of size at least c times the minimal index of a proper subgroup of G. There has been extensive investigation into clique size of these generating graphs, see for example [21], [44], [45] and [53]. However cocliques have been much less studied. In [50] Saunders proves that for each odd prime p, a maximal coclique in the generating graph of $\mathrm{PSL}_2(p)$ is either a maximal subgroup, or the conjugacy class of all involutions, or has size at most $\frac{129}{2}(p - 1) + 2$. In Chapters 5 and 6 we investigate when the intransitive and imprimitive maximal subgroups of the symmetric and alternating groups are maximal cocliques.

We begin with the definition of cliques and cocliques in arbitrary graphs.

Definition 4.5.1. Let $\mathcal{G}$ be a graph with vertex set V and edge set E, and let $U \subseteq V$.

The *induced subgraph* is the subgraph $\mathcal{G}_U$ of $\mathcal{G}$ with vertex set U and edge set

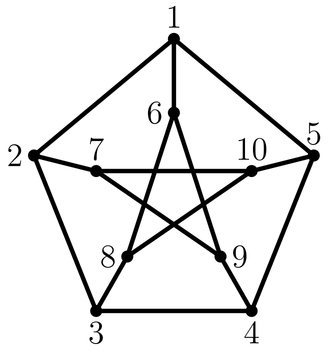
$$E_U = \big\{\{u, v\} \in E \mid u, v \in U\big\}.$$

A vertex $u \in V$ is *isolated* if it is adjacent to no other vertex. Equivalently u is isolated if $E_{\{u,v\}} = \emptyset$ for all $v \in V$.

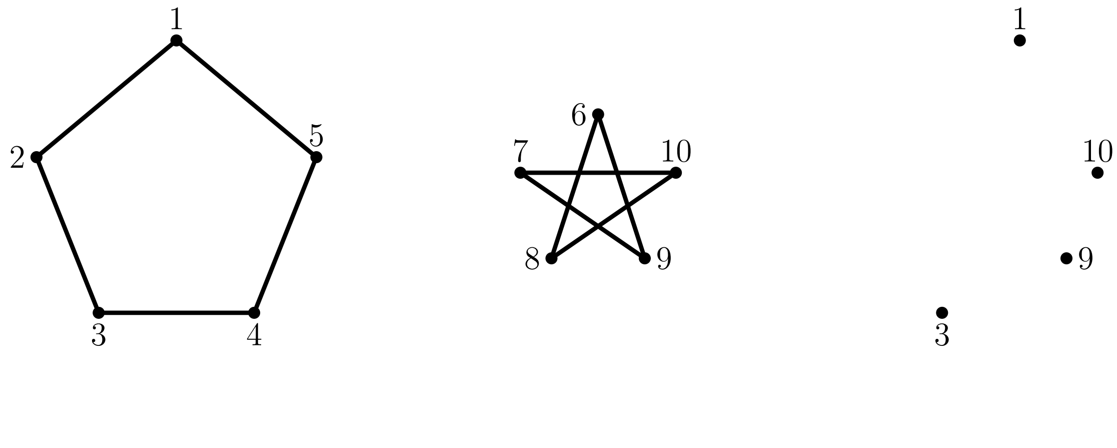
We call U a *coclique* of $\mathcal{G}$ if $\mathcal{G}_U$ is an empty induced subgraph, meaning that all vertices in $\mathcal{G}_U$ are isolated and so $E_U = \emptyset$. We call U a *clique* if $\mathcal{G}_U$ is a complete subgraph, that is $\{u, v\} \in E_U$ for all distinct $u, v \in U$.

A coclique is *maximal* if it is contained in no larger coclique, and similarly for cliques.

Example 4.5.2. The following graph $\mathcal{G} = (V, E)$ is the Petersen graph.



Let $S = \{1, 2, 3, 4, 5\}, T = \{6, 7, 8, 9, 10\}, U = \{1, 3, 9, 10\} \subseteq V$. Then the induced graphs, $\mathcal{G}_S$, $\mathcal{G}_T$ and $\mathcal{G}_U$, are as follows.



$\mathcal{G}_S$ $\mathcal{G}_T$ $\mathcal{G}_U$

Then S and T are neither cliques nor cocliques, and U is a coclique. Since $\mathcal{G}$ is triangle-free, it follows that cliques have size at most 2. We show that U is a maximal coclique using two different methods: one checks directly; and one which illustrates some interesting theoretical results.

First we use a direct method. From $U = \{1, 3, 9, 10\}$ it follows that $V \backslash U = \{2, 4, 5, 6, 7, 8\}$. Then $U \cup \{2\}$ is not a coclique since $1 \in U$ and $\{1, 2\} \in E$. Similarly $U \cup \{a\}$ is not a coclique for all $a \in V \backslash U$ since

$$\{4, 3\}, \{5, 10\}, \{6, 1\}, \{7, 9\}, \{8, 10\} \in E.$$

Hence U is contained in no larger coclique, and so U is a maximal coclique. △

We now show that the size of any coclique is at most four, and so U can be contained in no larger coclique. We begin with some theory.

For a graph $\mathcal{G} = (V, E)$, the *adjacency matrix* $A = (a_{ij})$ is the $|V| \times |V|$ matrix with $a_{ij} = 1$ if $\{i, j\} \in E$, and $a_{ij} = 0$ otherwise. The *inertia* of a matrix A is (a_+, a_-, a_0) where a_+, a_- and a_0 are the number of positive, negative and zero eigenvalues of A respectively.

Theorem 4.5.3 (Inertia Theorem [22]). *Let $\mathcal{G} = (V, E)$ be a graph, let $n = |V|$, and let (a_+, a_-, a_0) be the inertia of the adjacency matrix of $\mathcal{G}$. Then the size of any coclique in $\mathcal{G}$ is at most*

$$\min\{n - a_+, n - a_-\}.$$

Example 4.5.4. Let the Petersen graph be labelled as in Example 4.5.2. The adjacency matrix corresponding to this labelling is as follows

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

It can be verified that A has eigenvalues 1 with multiplicity five, 3 with multiplicity one, and -2 with multiplicity four. Thus the inertia of A is $(6, 4, 0)$, and so by Theorem 4.5.3 any coclique of $\mathcal{G}$ has size at most 4. Hence U is a maximal coclique. △

We now give the definition of a generating graph, first defined by Liebeck and Shalev in [42].

Definition 4.5.5. Let G be a 2-generated group. The *generating graph* of G, denoted

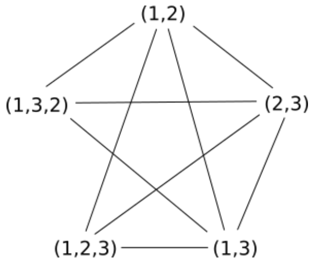
$\Gamma(G)$, has vertex set $G\backslash\{1\}$, and edge set $\big\{\{x,y\} \mid \langle x,y\rangle = G\big\}$.

Some sources take all elements of G as the vertex set of $\Gamma(G)$, and so the identity is an isolated vertex, however we do not do this here.

Let G be a finite group with proper subgroup H and generating graph $\Gamma(G)$. Then for all $x, y \in H$ it follows that $\langle x,y\rangle \leq H$. Hence the elements of $H\backslash\{1\}$ form a coclique in $\Gamma(G)$. In a slight abuse of language (since we do not consider the identity element to be a vertex), we say that H is a coclique in $\Gamma(G)$. Therefore each maximal subgroup of G is a coclique in $\Gamma(G)$, but it may not be a maximal coclique. This observation prompts our investigations in Chapters 5 and 6.

We now consider some of generating graphs with maximal and non-maximal examples of cliques and cocliques.

Example 4.5.6. Let $G = \mathrm{S}_3$ so that $\Gamma(G) = (V, E)$ is as follows.



Then $\big\{(1,3,2),(1,2,3)\big\} \notin E$, since $\big\langle(1,3,2),(1,2,3)\big\rangle$ is a proper subgroup of G. Hence $U = \{(1,3,2),(1,2,3)\}$ is a coclique in $\Gamma(G)$. Since both $(1,3,2)$ and $(1,2,3)$ are connected to every vertex of $V\backslash U$, it follows that U is a maximal coclique.

Let $R = \{(1,2),(2,3),(1,3),(1,2,3)\}$ and $S = \{(1,2),(2,3),(1,3),(1,3,2)\}$. Then $\Gamma(G)_R$ and $\Gamma(G)_S$ are both complete graphs on 4 points. Hence R and S are cliques. Because $\big\{(1,3,2),(1,2,3)\big\} \notin E$, it follows that $R \cup \{(1,3,2)\}$ and $S \cup \{(1,2,3)\}$ are not cliques. Therefore R and S are maximal cliques. △

Example 4.5.7. Let $G = \mathrm{S}_4$, and let $\Gamma(G) = (V, E)$ be the generating graph of G. Then $\langle(2,3,4),(2,3)\rangle \cong \mathrm{S}_3$ and $\langle(1,2,3,4),(1,2)(3,4)\rangle \cong \mathrm{Dih}(8)$ are maximal subgroups of G, and so $U_1 = \mathrm{S}_3\backslash\{1\}$ and $U_2 = \mathrm{Dih}(8)\backslash\{1\}$ are cocliques in $\Gamma(G)$.

We introduce the following notation which will help to visualise whether or not U_1 and U_2 are maximal cocliques in $\Gamma(G)$. For $i = 1$ or 2, let

$$E_i = \big\{\{x,y\} \in E \mid x \in U_i, y \notin U_i\big\},$$

and let $\mathcal{G}_i = (V, E_i)$. The following figures show $\mathcal{G}_1$ and $\mathcal{G}_2$ with U_1 and U_2 highlighted.

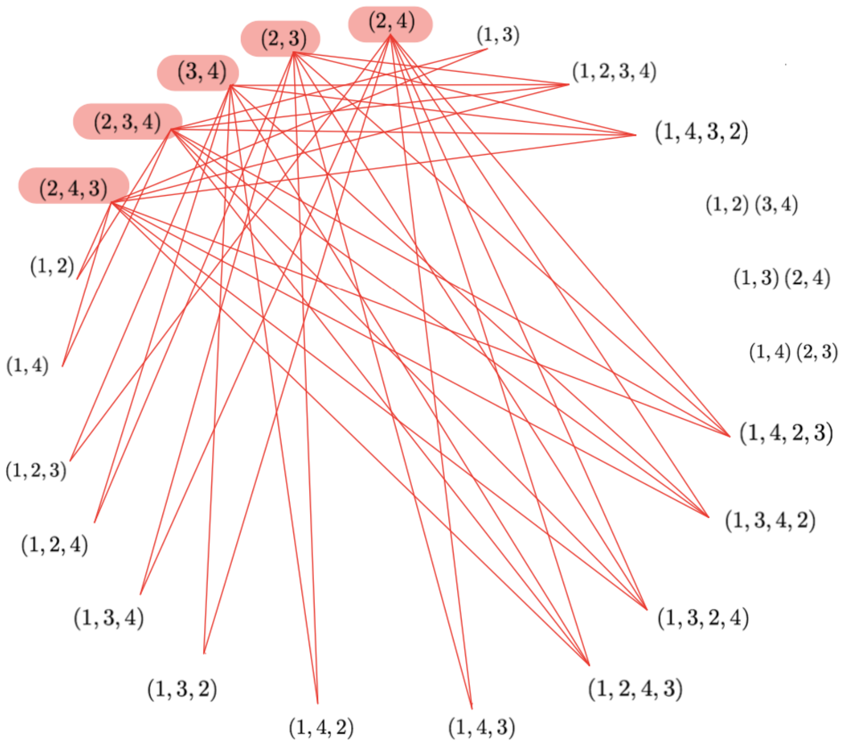


Figure 4.1: $\mathcal{G}_1$

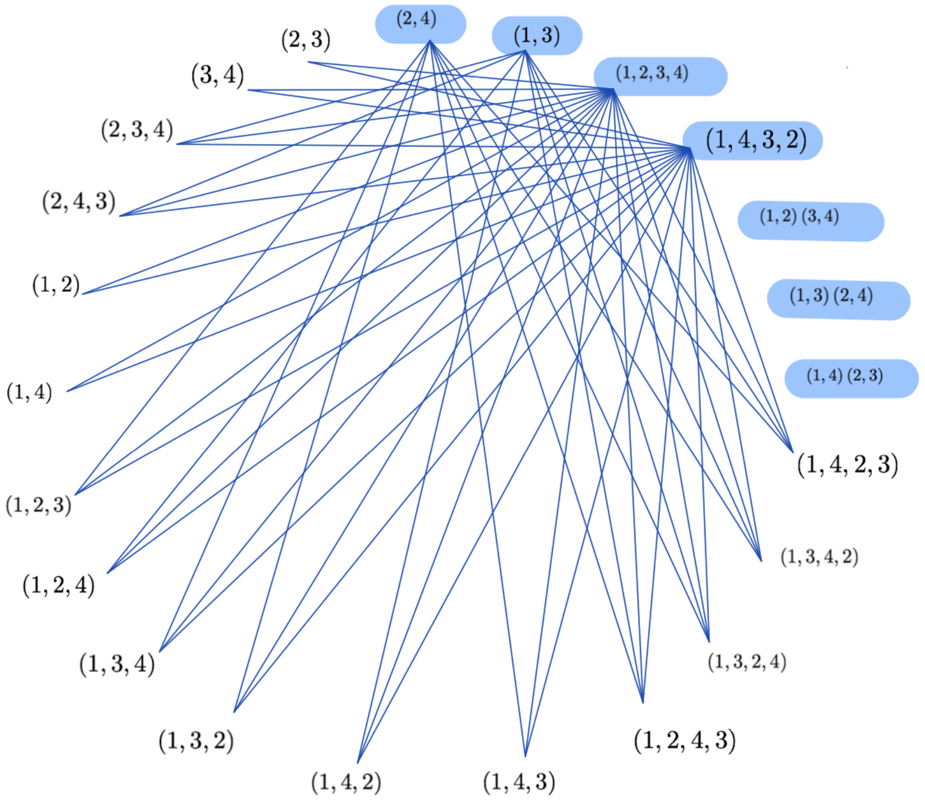


Figure 4.2: $\mathcal{G}_2$

In Figure 4.1, $(1,3)(2,4) \in V\backslash U_1$ is not connected to any element in U_1, and so $\{U_1, (1,3)(2,4)\}$ is a coclique in $\Gamma(G)$ containing U_1. Hence U_1 is not a maximal coclique. Each element of $V\backslash U_2$ is connected to some element in U_2. Therefore U_2 is a maximal coclique. △

Since the examples above are small, it was easy to verify them directly. We now show one possible way that theoretical arguments can be used to identify maximal cocliques in generating graphs. We begin with some background material.

Definition 4.5.8. Let G be a finite group. The *Frattini subgroup* of G, $\Phi(G)$, is the intersection of all maximal subgroups of G.

The following lemma illustrates why the Frattini subgroup is sometimes called the non-generating subgroup.

Lemma 4.5.9. *Let G be a group and let $X \subseteq G$. If $\langle X, \Phi(G)\rangle = G$, then $\langle X\rangle = G$.*

Proof. Let $X \subseteq G$ such that $\langle X, \Phi(G)\rangle = G$ and $\langle X\rangle \neq G$. Then $\langle X\rangle$ is a proper subgroup of G, and so is contained in some maximal subgroup M of G. Therefore, $\langle X, \Phi(G)\rangle \leq M < G$, contradicting the initial assumption. □

Let p be a prime. An *elementary abelian p-group* is an abelian group in which every non-trivial element has order p.

Theorem 4.5.10 (Burnside's Basis Theorem [54, Theorem 1.16])**.** *Let p be a prime and let G be a d-generated p-group. Then $G/\Phi(G)$ is an elementary abelian p-group of order p^d.*

Theorem 4.5.11. *Let p be a prime and let G be a 2-generated p-group. Then the maximal subgroups of G are maximal cocliques in $\Gamma(G)$.*

Proof. Let M be a maximal subgroup of G and let $x \in G\backslash M$. Since $x \notin M$ it follows that x lies in a maximal subgroup $N \neq M$, and so $\Phi(G) \leq M \cap N < M$. Hence there exists $y \in M\backslash\Phi(G)$. We now show that $\langle x, y\rangle = G$, and so the result holds.

Let $Q := G/\Phi(G)$ and let $[x] = x\Phi(G), [y] = y\Phi(G) \in Q$. Then $[x], [y] \neq [1]$, since $y \in M\backslash\Phi(G)$ and $x \notin M > \Phi(G)$. Hence by Theorem 4.5.10, $[x]$ and $[y]$ have order p.

Suppose for a contradiction that $[x] \in \langle [y]\rangle$. Then there exists $a \in \mathbb{N}$ such that $[x] = [y]^a$. Therefore $[1] = [xy^{-a}]$, and so $xy^{-a} \in \Phi(G) \leq M$. A contradiction since $y \in M$ and $x \notin M$.

Since $[y]$ has order p and Q has order p^2, it follows that $\langle [y]\rangle$ is a maximal subgroup of Q. Therefore $\langle [x], [y]\rangle = Q$, and so $G = \langle x, y\rangle\Phi(G) = \langle x, y, \Phi(G)\rangle$. By Lemma 4.5.9, it follows that $G = \langle x, y, \Phi(G)\rangle = \langle x, y\rangle$. □

In [14] Cameron, Lucchini and Roney-Dougal defined the following equivalence relation. We prove a related result in Chapter 5.

Definition 4.5.12. Let G be a finite group and let $x, y \in G$. Then $x \equiv_m y$ if and only if x and y can be substituted for one another in all generating sets for G, and $x \equiv_m^{(r)} y$ exactly when x and y can be substituted for one another in any generating set of size r. Finally, let $\psi(G)$ be the minimal value of r at which $\equiv_m^{(r)}$ and $\equiv_m$ are the same equivalence relation.

Example 4.5.13. Let $G = \mathrm{S}_3$. As can be seen in the generating graph given in Example 4.5.6 the elements $(1,2,3)$ and $(1,3,2)$ have the same set of neighbours, and so $(1,2,3) \equiv_m^{(2)} (1,3,2)$ △

4.6 General results on S_n and affine groups

In Chapter 5 we show the following. Let $p \geq 5$ be a prime such that $p \neq \frac{q^d-1}{q-1}$ for all prime powers q and $d \geq 2$. We shall prove that all maximal subgroups of S_p are maximal cocliques in $\Gamma(\mathrm{S}_p)$; and for $p > 5$ all maximal subgroups of A_p are maximal cocliques in $\Gamma(\mathrm{A}_p)$. As part of the proof we show that the one-dimensional affine groups (see Definition 4.6.5) are maximal cocliques in S_p. Here we introduce the affine groups and prove some lemmas which we use in Chapter 5. We begin with a definition and lemma for arbitrary groups, and then two lemmas concerning S_n.

Definition 4.6.1. Let G be a group with subgroup H. Then H is *self-normalizing* in G if $\mathrm{N}_G(H) = H$.

Lemma 4.6.2. *Let G be a finite group, let H be a self-normalizing subgroup of G and let $x \in G$. Then the number of cosets of H in G which are stabilized by x in right coset action is equal to the number of conjugates of H in G which contain x.*

Proof. Let $g_1, g_2 \in G$. Then

$$H^{g_1} = H^{g_2} \iff H^{g_1 g_2^{-1}} = H \iff g_1 g_2^{-1} \in \mathrm{N}_G(H) = H \iff Hg_1 = Hg_2.$$

Hence there exists a set $\{g_1, \ldots, g_r\} \subseteq G$ of representative elements for both the cosets of H and the G-conjugates of H. Then for $1 \leq i \leq r$

$$Hg_i x = Hg_i \iff Hg_i x g_i^{-1} = H \iff g_i x g_i^{-1} \in H \iff x \in g_i^{-1} H g_i = H^{g_i}. \quad \square$$

Lemma 4.6.3. *Let $G = \mathrm{S}_n$ and let $g, h \in G$ be two n-cycles. Then there are exactly n elements of G conjugating g to h.*

Proof. Let $g = (a_0, a_1, \dots, a_{n-1})$, let $h = (b_0, b_1, \dots, b_{n-1})$ and let $k \in \mathrm{S}_n$. Then

$$k^{-1}gk = \left(a_0^k, a_1^k, \dots, a_{n-1}^k\right).$$

Since $\Omega = \{a_0, \dots, a_{n-1}\} = \{b_0, \dots, b_{n-1}\}$ there exists $0 \leq i \leq n-1$ such that $a_0^k = b_i$. Hence if $k^{-1}gk = h$, then $a_j^k = b_{i+j}$ for $0 \leq j \leq n$ with subscripts taken modulo n. Hence for fixed i, there is exactly one $k \in \mathrm{S}_n$ such that $g^k = h$ and $a_0^k = b_i$. Since there are n possibilities for a_0^k the result follows. □

Lemma 4.6.4. *Let $p \geq 5$, let $G = \mathrm{S}_p$, let $M = \mathrm{A}_p$. For all $x \in G \backslash M$, there exists a p-cycle $y \in M$ such that y is not normalized by x.*

Proof. Let y be a p-cycle and let $\alpha \in \Omega = \{1, 2, \dots, p\}$. If $z \in \langle y \rangle$ and $\alpha^z = \alpha^{y^i}$ for some $i \in \mathbb{Z}$, then $z = y^i$.

If $|\mathrm{Fix}(x)| \geq 2$, then there exists $\alpha, \beta \in \mathrm{Fix}(x)$. Let $\gamma \in \mathrm{Supp}(x)$. Let y be a p-cycle with $\alpha^y = \beta$ and $\alpha^{y^2} = \gamma$. Then

$$\alpha^{x^{-1}yx} = \alpha^{yx} = \beta^x = \beta = \alpha^y \quad \text{and} \quad \alpha^{(x^{-1}yx)^2} = \beta^{x^{-1}yx} = \beta^{yx} = \gamma^x \neq \gamma = \alpha^{y^2}.$$

Hence $\alpha^{y^x} = \alpha^y$ and $\alpha^{(y^x)^2} \neq \alpha^{y^2}$. Therefore $y^x \notin \langle y \rangle$, and so x does not normalise y.

Hence we may assume that $|\mathrm{Fix}(x)| \leq 1$. Since $p \geq 5$ it follows that $|\mathrm{Supp}(x)| \geq 4$, and so the disjoint cycle decomposition of x contains either a product of two transpositions, a 3-cycle, or an r-cycle for $r \geq 4$.

First assume that x contains a product of two transpositions, which we label $(\alpha, \beta)(\gamma, \delta)$. Let $\epsilon \in \{1, \dots, p\} \backslash \{\alpha, \beta, \gamma, \delta\}$ and let y be a p-cycle with $\alpha^y = \beta$, $\beta^y = \gamma$ and $\alpha^{y^{-1}} = \epsilon$. Then

$$\beta^{x^{-1}yx} = \alpha^{yx} = \beta^x = \alpha = \beta^{y^{-1}} \quad \text{and} \quad \alpha^{x^{-1}yx} = \beta^{yx} = \gamma^x = \delta \neq \epsilon = \alpha^{y^{-1}}.$$

Hence $y^x \notin \langle y \rangle$, and so x does not normalise y.

Next assume that x contains a 3-cycle which we label (α, β, γ). Let y be a p-cycle with $\alpha^y = \beta$ and $\beta^y = \gamma$. Then $\alpha^{y^2} = \gamma$, and since $p \geq 5$ it follows that $\gamma^y \neq \alpha$. Then

$$\beta^{x^{-1}yx} = \alpha^{yx} = \beta^x = \gamma = \beta^y \quad \text{and} \quad \gamma^{x^{-1}yx} = \beta^{yx} = \gamma^x = \alpha \neq \gamma^y.$$

Hence $y^x \notin \langle y \rangle$, and so x does not normalise y.

Finally suppose that x contains an r-cycle with $r \geq 4$. Hence there exist $\alpha, \beta, \gamma, \delta \in \mathrm{Supp}(x)$ with $\alpha^x = \beta$, $\beta^x = \gamma$ and $\gamma^x = \delta$. Let $\epsilon \in \{1, \ldots, p\} \backslash \{\alpha, \beta, \gamma, \delta\}$, and let y be a p-cycle with $\alpha^y = \beta$, $\beta^y = \gamma$ and $\gamma^y = \epsilon$. Then

$$\beta^{x^{-1}yx} = \alpha^{yx} = \beta^x = \gamma = \beta^y \quad \text{and} \quad \gamma^{x^{-1}yx} = \beta^{yx} = \gamma^x = \delta \neq \epsilon = \gamma^y.$$

Hence $y^x \notin \langle y \rangle$, and so x does not normalise y. □

We now introduce the affine groups. For the remainder of this section let p be a prime, let $\mathbb{F} = \mathrm{GF}(p)$ and $\mathbb{F}^* = \mathbb{F} \backslash \{0\}$, and let $\alpha \in \mathbb{F}^*$ and $\beta \in \mathbb{F}$. Then we can define a map $t_{\alpha,\beta} : \mathbb{F} \to \mathbb{F}$ by

$$t_{\alpha,\beta} : \xi \mapsto \alpha\xi + \beta \quad \text{for } \xi \in \mathbb{F}.$$

We call such a function a *1-dimensional affine transformation.* We show that the collection of all 1-dimensional affine transformations forms a group under composition of maps.

Let $\alpha, \alpha' \in \mathbb{F}^*$ and let $\beta, \beta', \xi \in \mathbb{F}$. Then $\alpha\alpha' \in \mathbb{F}^*$ and

$$\begin{aligned} t_{\alpha,\beta} t_{\alpha',\beta'}(\xi) &= t_{\alpha,\beta}(\alpha'\xi + \beta') \\ &= \alpha(\alpha'\xi + \beta') + \beta \\ &= \alpha\alpha'\xi + \alpha\beta' + \beta. \end{aligned} \tag{4.9}$$

Hence $t_{\alpha,\beta} t_{\alpha',\beta'} = t_{\alpha\alpha',\alpha\beta'+\beta}$ is a 1-dimensional affine transformation. From $t_{1,0}(\xi) = 1\xi + 0$ for all $\xi \in \mathbb{F}$, it follows that $t_{1,0}$ acts as the identity map on $\mathbb{F}$. Since $\alpha \in \mathbb{F}^*$ it follows that $\alpha^{-1} \in \mathbb{F}^*$. Hence $t_{\alpha^{-1},-\alpha^{-1}\beta}$ is a 1-dimensional affine transformation and $t_{\alpha,\beta}^{-1} = t_{\alpha^{-1},-\alpha^{-1}\beta}$ by (4.9). Since composition of maps is associative, it follows that we may define the following subgroup of $\mathrm{Sym}(\mathbb{F})$.

Definition 4.6.5. The *1-dimensional affine group* is

$$\mathrm{AGL}_1(\mathbb{F}) = \{t_{\alpha,\beta} \mid \alpha \in \mathbb{F}^* \text{ and } \beta \in \mathbb{F}\}.$$

Up to isomorphism $\mathrm{GF}(p)$ is the only field of order p. Hence we may write $\mathrm{AGL}_1(p) \leq \mathrm{Sym}(\mathrm{GF}(p)) \cong \mathrm{S}_p$ in place of $\mathrm{AGL}_1(\mathbb{F}) \leq \mathrm{Sym}(\mathbb{F})$.

Let $\alpha, \alpha' \in \mathbb{F}^*$ and $\beta, \beta' \in \mathbb{F}$. If $\beta \neq \beta'$, then

$$t_{\alpha,\beta}(0) = \beta \neq \beta' = t_{\alpha',\beta'}(0).$$

If $\beta = \beta'$ and $\alpha \neq \alpha'$, then

$$t_{\alpha,\beta}(1) = \alpha + \beta \neq \alpha' + \beta' = t_{\alpha',\beta'}(1).$$

Hence $t_{\alpha,\beta} = t_{\alpha',\beta'}$ if and only if $(\alpha, \beta) = (\alpha', \beta')$. Therefore $|\mathrm{AGL}_1(p)| = (p-1)p$.

We now introduce two subgroups of $\mathrm{AGL}_1(p)$ and prove some results about these subgroups. Let $G = \mathrm{AGL}_1(p)$, let $T = \{t_{1,\gamma} \mid \gamma \in \mathbb{F}\}$ and let $R = \{t_{\alpha,0} \mid \alpha \in \mathbb{F}^*\}$.

Lemma 4.6.6. *Let G and T be as above. Then T is a regular normal subgroup of G.*

Proof. Let $t_{1,\gamma}, t_{1,\gamma'} \in T$. Then $t_{1,\gamma}t_{1,\gamma'} = t_{1,\gamma\gamma'} \in T$ and $t_{1,\gamma}^{-1} = t_{1,-\gamma} \in T$, and so $T \leq G$. Since $t_{1,\gamma} = t_{1,1}^{\gamma}$ it follows that $T = \langle t_{1,1} \rangle \cong C_p$. Let $t_{\alpha,\beta} \in G$ and $t_{1,\gamma} \in T$. Then for $\xi \in \mathbb{F}$

$$\begin{aligned}
t_{\alpha,\beta}^{-1} t_{1,\gamma} t_{\alpha,\beta}(\xi) &= t_{\alpha^{-1},-\alpha^{-1}\beta} t_{1,\gamma} t_{\alpha,\beta}(\xi) \\
&= t_{\alpha^{-1},-\alpha^{-1}\beta} t_{1,\gamma}(\alpha\xi + \beta) \\
&= t_{\alpha^{-1},-\alpha^{-1}\beta}(\alpha\xi + \beta + \gamma) \\
&= \alpha^{-1}(\alpha\xi + \beta + \gamma) - \alpha^{-1}\beta \\
&= \xi + \alpha^{-1}\gamma \\
&= t_{1,\alpha^{-1}\gamma}(\xi).
\end{aligned}$$

Now $t_{1,\alpha^{-1}\gamma} \in T$, and so $T \trianglelefteq G$. □

Lemma 4.6.7. *Let G, T and R be as above. Then $G = T \rtimes R$.*

Proof. Let $t_{\alpha,0}, t_{\alpha',0} \in R$. Then $t_{\alpha,0}t_{\alpha',0} = t_{\alpha\alpha',0} \in R$ and $t_{\alpha,0}^{-1} = t_{\alpha^{-1},0} \in R$, and so $R \leq G$. Clearly $T \cap R = \{t_{1,0}\} = \{\mathrm{id}\}$. Let $t_{\alpha,\beta} \in G$. Then

$$t_{\alpha,\beta}(\xi) = \alpha\xi + \beta = t_{1,\beta}(\alpha\xi) = t_{1,\beta}t_{\alpha,0}(\xi),$$

with $t_{1,\beta} \in T$ and $t_{\alpha,0} \in R$. Hence $G = TR$. □

We now collect some results about $\mathrm{AGL}_1(p)$ which will be used in Chapter 5.

Lemma 4.6.8. *Let $S = \mathrm{Sym}(\mathbb{F})$, let $G = \mathrm{AGL}_1(p) \leq S$ and let $T = \langle t_{11} \rangle \trianglelefteq G$. Then the following hold.*

(i) *The group G is sharply 2-transitive.*

(ii) *Each element of G is either a p-cycle or a power of a $(p-1)$-cycle.*

(iii) *For all $\xi \in \mathbb{F}$, there exists a $(p-1)$-cycle $z \in G$ fixing ξ.*

(iv) *The group of translates, $T = \langle t_{11} \rangle$, is the unique Sylow p-subgroup of G and $G = \mathrm{N}_S(T)$.*

(v) *If $y_1, y_2 \in G$ are $(p-1)$-cycles and $\langle y_1 \rangle \neq \langle y_2 \rangle$, then $G = \langle y_1, y_2 \rangle$.*

Proof. (i) To show that G is sharply 2-transitive we show that for all $\gamma, \delta \in \mathbb{F}^*$ there exists a unique $t \in G$ such that $t(0) = 0$ and $t(\gamma) = \delta$.

Let $t := t_{\alpha,\beta} \in G$. Then $t(0) = 0 + \beta$, and so $t(0) = 0$ if and only if $\beta = 0$. Now let $t := t_{\alpha,0}$. Then $t(\gamma) = \alpha\gamma$, and so $t(\gamma) = \delta$ if and only if $\alpha = \delta\gamma^{-1}$. Therefore the result follows.

(ii)-(iii) We begin by finding a $(p-1)$-cycle in G. Let ω be a primitive element of $\mathbb{F}^*$, let $\gamma \in \mathbb{F}$ and let $r := t_{\omega,\gamma} \in G$. Then for $i \in \mathbb{N}$ and $\xi \in \mathbb{F}$

$$\begin{aligned} r^i(\xi) &= \omega^i\xi + \gamma(\omega^{i-1} + \omega^{i-2} + \cdots + \omega + 1) \\ &= \omega^i\xi + \gamma(\omega^i - 1)(\omega - 1)^{-1} \qquad (4.10) \\ &= t_{\omega^i,\gamma(\omega^i-1)(\omega-1)^{-1}}(\xi). \end{aligned}$$

Since ω has order $p-1$, it follows that $r^i \neq t_{1,0}$ for $i < p-1$ and that $r^{p-1} = t_{1,0}$. Hence r has order $p-1$.

If $r^i(\xi) = \xi$, then $\xi(1-\omega^i) = \gamma(\omega^i - 1)(\omega-1)^{-1}$ by (4.10), and so $\xi = \gamma(1-\omega)^{-1}$. Therefore, for $1 \leq i \leq p-1$, the only fixed point of r^i is $\gamma(1-\omega)^{-1}$. Hence from $G \leq S$, it follows that r is a $(p-1)$-cycle. Thus for $\epsilon \in \mathbb{F}$ it follows that $t_{\omega,\epsilon(1-\omega)}$ is a $(p-1)$-cycle fixing ϵ, and so (iii) follows.

By The Orbit-Stabilizer Theorem $|G_0| = p-1$, and by the above $t_{\omega,0}$ is a $(p-1)$-cycle. Hence $G_0 = \langle t_{\omega,0}\rangle$. Since G is transitive it follows that all point stabilizers are conjugate. Hence if $t \in G$ has a fixed point, then t is a power of a $(p-1)$-cycle.

If $t \in G \backslash T$ then $t = t_{\alpha,\beta}$ for $\alpha \neq 0, 1$. Hence $t \neq \mathrm{id}$ fixes $\beta(1-\alpha)^{-1}$ and so is a power of a $(p-1)$-cycle. If $T \in T\backslash\{1\} \cong C_p\backslash\{1\}$ then t is a p-cycle.

(iv) Since $|G| = p(p-1)$ and $|T| = p$ it follows that T is a Sylow p-subgroup for G. By Sylow's Theorem all Sylow p-subgroups are conjugate, hence T is the unique Sylow p-subgroup by Lemma 4.6.6.

If an element of S normalizes T, then it maps $t_{1,1}$ to one of $p-1$ non-trivial elements of T, namely $t_{1,1}, t_{1,1}^2, \ldots, t_{1,1}^{(p-1)}$. By Lemma 4.6.3, for fixed $1 \leq i \leq p-1$, there are exactly p elements of S which conjugate $t_{1,1}$ to $t_{1,1}^i$. Therefore $|\mathrm{N}_S(T)| = p(p-1) = |G|$. Since $T \trianglelefteq G$ it follows that $G \leq \mathrm{N}_S(T)$, and so $G = \mathrm{N}_S(T)$.

(v) Let $y_1, y_2 \in G$ be $(p-1)$-cycles such that $\langle y_1\rangle \neq \langle y_2\rangle$. Hence $[G : \langle y_1\rangle] = p$, and so $\langle y_1\rangle$ is a maximal subgroup of G. Since $y_2 \notin \langle y_1\rangle$ it follows that $\langle y_1, y_2\rangle = G$. □

Chapter 5

Intransitive subgroups as cocliques

Let G be $\mathrm{S}_n := \mathrm{Sym}(\{1,\dots,n\})$ or $\mathrm{A}_n := \mathrm{Alt}(\{1,\dots,n\})$, let M be an intransitive maximal subgroup of G and let $\Gamma(G)$ be the generating graph of G. Recall that for ease we say that M is a maximal coclique if $M\backslash\{1\}$ is a maximal coclique in $\Gamma(G)$.

As discussed in Section 4.5, M is a coclique in $\Gamma(G)$, but not necessarily a maximal coclique. Here we determine when M is a maximal coclique on $\Gamma(G)$, and when M is not we find the unique maximal coclique containing M.

In addition, we prove a conjecture of Cameron, Lucchini and Roney-Dougal [14] holds for G under certain conditions on n. The results of this chapter are stated in full in the following section.

The material in this chapter is from [34], with more detail given here.

5.1 Introduction

Our first main theorem determines when M is a maximal coclique.

Theorem 5.1.1. *Let $n \geq 4$, let $G = \mathrm{S}_n$ or A_n, let $n > k > \frac{n}{2}$ and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$ be an intransitive maximal subgroup of G.*

(i) *If $G = \mathrm{S}_n$, then M is a maximal coclique in $\Gamma(G)$ if and only if $\gcd(n,k) = 1$ and $(n,k) \neq (4,3)$.*

(ii) *If $G = \mathrm{A}_n$, then M is a maximal coclique in $\Gamma(G)$ if and only if $(n,k) \notin \{(5,3),(6,4)\}$.*

The following concerns the exceptional cases of Theorem 5.1.1.

Theorem 5.1.2. (i) *Let $n \geq 4$, let $G = \mathrm{S}_n$, let $n > k > \frac{n}{2}$ and let $M = \mathrm{S}_k \times \mathrm{S}_{n-k}$ be the intransitive maximal subgroup of G stabilizing $\{1,\dots,k\}$ setwise.*

(a) *If* $\gcd(n,k) > 1$*, then the unique maximal coclique of* $\Gamma(G)$ *containing* M *is* $M \cup (1,k+1)^M \backslash \{1\}$.

(b) *If* $(n,k) = (4,3)$*, then the unique maximal coclique of* $\Gamma(G)$ *containing* M *is* $M \cup (1,4)(2,3)^M \backslash \{1\}$.

(ii) *Let* $(n,k) \in \{(5,3),(6,4)\}$*, let* $G = \mathrm{A}_n$ *and let* $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$ *be the intransitive maximal subgroup of* G *stabilizing* $\{1,\dots,k\}$ *setwise.*

(a) *If* $(n,k) = (5,3)$*, then the unique maximal coclique of* $\Gamma(G)$ *containing* M *is* $M \cup (1,4)(2,3)^M \backslash \{1\}$.

(b) *If* $(n,k) = (6,4)$*, then the unique maximal coclique of* $\Gamma(G)$ *containing* M *is* $M \cup (1,5)(2,6)^M \backslash \{1\}$.

Recall by Definition 4.5.1, that a vertex of a graph is isolated if it has no neighbours. Settling a long-standing conjecture, Burness, Guralnick and Harper show in [8] that if G is a finite group of order greater than two and all proper quotients of G are cyclic, then no vertex of $\Gamma(G)$ is isolated. The result for $G = \mathrm{A}_n$ and S_n goes back much further, see [48].

Let G be a finite group, let $x, y \in G$, and let $\equiv_m^{(r)}$, $\equiv_m$ and ψ be as in Definition 4.5.12. Hence $\psi(G) \leq 2$, if $x \equiv_m^{(2)} y$ implies that $x \equiv_m y$. In [14], Cameron Lucchini and Roney-Dougal make the following conjecture.

Conjecture 5.1.3 ([14, Conjecture 4.7])**.** *Let* G *be a finite group such that no vertex of* $\Gamma(G)$ *is isolated. Then* $\psi(G) \leq 2$.

The authors observe on p14 that as a consequence their Lemma 2.17 in the same paper, that to prove Conjecture 5.1.3, it suffices to show that each maximal subgroup is a maximal coclique in $\Gamma(G)$. This motivates the following theorem.

Theorem 5.1.4. *Let* $p \geq 5$ *be a prime such that* $p \neq \frac{q^d-1}{q-1}$ *for all prime powers* q *and all* $d \geq 2$*, and let* $G = \mathrm{S}_p$ *or* A_p.

(i) *If* $G = \mathrm{S}_p$*, then each maximal subgroup of* G *is a maximal coclique in* $\Gamma(G)$.

(ii) *If* $G = \mathrm{A}_p$*, then each maximal subgroup* M *of* G *is a maximal coclique in* $\Gamma(G)$ *except when* $p = 5$ *and* $M = (\mathrm{S}_3 \times \mathrm{S}_2) \cap G$.

The restrictions on p, when combined with Theorem 5.4.1, enable us to fully describe the transitive subgroups of S_p. For more discussion see Chapter 7.

Theorem 2.26 of [14] states that $\psi(\mathrm{A}_5) = 2$. Hence, using the authors' observation the following is immediate and verifies Conjecture 5.1.3 for S_p and A_p when $p \neq \frac{q^d-1}{q-1}$.

Corollary 5.1.5. *Let G and p be as in Theorem 5.1.4. Then $\psi(G) = 2$. That is, two elements of G belong to exactly the same maximal subgroups of G if and only if they can be substituted for each other in all generating pairs for G.*

This chapter is structured as follows. In Section 5.2 we prove some preliminary lemmas and show that Theorems 5.1.1 and 5.1.2 hold for $n \leq 11$. In Section 5.3 we complete the proof of Theorems 5.1.1 and 5.1.2. Finally, in Section 5.4 we prove Theorem 5.1.4. Some small cases, which are proved primarily using Magma, are covered in the appendix, Chapter 8.

5.2 Preliminary results

We begin by introducing some notation and preliminary lemmas which we use for the remainder of the chapter. We then show that Theorems 5.1.1 and 5.1.2(i) hold when $n \leq 11$, and prove Theorem 5.1.2(ii). Finally we divide the task of proving Theorems 5.1.1 and 5.1.2(i) into subcases.

Throughout this and the next section we use the following notation.

Notation 5.2.1. Let $n > k > \frac{n}{2} \geq 2$ and let $\Omega = \Omega_1 \cup \Omega_2 = \{1, \dots, k\} \cup \{k+1, \dots, n\}$. Let $G = \mathrm{S}_n$ or A_n acting on Ω, let

$$M = \mathrm{Stab}_G(\Omega_1) = \mathrm{Stab}_G(\Omega_2) \cong \Big(\mathrm{S}_k \times \mathrm{S}_{n-k}\Big) \cap G,$$

and let $x \in G \backslash M$. Let $\mathcal{J}_t, \mathcal{J}_c$ and $\mathcal{J}_s$ be as in Definition 4.3.3, and let $\mathcal{J}$ be as in Theorem 4.3.4.

Recall that M is a maximal coclique in $\Gamma(G)$ if and only if for all $x \in G \backslash M$ there exists $y \in M$ such that $\langle x, y \rangle = G$. In the following we show that it suffices to consider x up to conjugation by M.

Lemma 5.2.2. *Let G and M be as in Notation 5.2.1. Let X be the set of elements of $G \backslash M$ up to conjugation by M. Then M is a maximal coclique in $\Gamma(G)$ if and only if for each $x \in X$ there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If M is a maximal coclique then for all $x \in G \backslash M$, and so in particular for all $x \in X \subseteq G \backslash M$, there exists $y \in M$ such that $\langle x, y \rangle = G$. Hence the forward direction holds.

Now assume that M is not a maximal coclique of $\Gamma(G)$. Then there exists $x_1 \in G \backslash M$ such that $\langle x_1, y \rangle \neq G$ for all $y \in M$. Let $m \in M$ and let $x := x_1^m$. Then for all $y \in M$ we deduce that

$$\langle x, y^m \rangle = \langle x_1^m, y^m \rangle \neq G^m = G. \quad \square$$

We now prove Theorem 5.1.1 for some small values of n and $n-k$.

Lemma 5.2.3. *Let $n \leq 11$. Then Theorems 5.1.1 and 5.1.2 hold.*

Proof. Let X be a list of all possibilities for $x \in G \backslash M$ up to M-conjugacy. For $x \in X$, let L_x be a list of elements of M up to conjugation by $C_M(x)$ (the centralizer of x in M).

If there exists $x \in X$ such that $\langle x, y\rangle \neq G$ for all $y \in M$, then $\langle x, y\rangle \neq G$ for all $y \in L_x$. If there exists $x \in X$ such that $\langle x, y\rangle \neq G$ for all $y \in L_x$, then $\langle x, y^c\rangle = \langle x^c, y^c\rangle \neq G^c = G$ for all $c \in C_M(x)$. Since $L_x^{C_M(x)} = M$, Lemma 5.2.2 implies that M is a maximal coclique if and only if for all $x \in X$ there exists $y \in L_x$ such that $\langle x, y\rangle = G$.

We proceed using [33, Code 1] in Magma, which we summarise here. For each n and each $n > k > \frac{k}{2}$ we construct X, and for each $x \in X$ we calculate the corresponding L_x. If there exists $y \in L_x$ such that $\langle x, y\rangle = G$ then remove x from X. Hence after this routine, M is a maximal coclique in $\Gamma(G)$ if and only if $X = \emptyset$.

There are a small number of cases of n, k and G for which $X \neq \emptyset$. We list them here along with $x \in X$.

(i) $G = \mathrm{S}_n$, $x = (1, k+1)$ and $(n, k) = (6,4)$, $(8,6)$, $(9,6)$, $(10,6)$ or $(10,8)$; or

(ii) $(G, k, x) = (\mathrm{S}_4, 3, (1,4)(2,3))$, $(\mathrm{A}_5, 3, (1,4)(2,3))$, or $(\mathrm{A}_6, 4, (1,5)(2,6))$.

Hence $\langle z, y\rangle \neq G$ for all $z \in x^M$ and $y \in M$. Any two elements of x^M are involutions and so generated a dihedral group. Therefore in these cases the maximal coclique in $\Gamma(G)$ containing M is $M \cup x^M \backslash \{1\}$. □

We now use Lemma 5.2.2 to prove an assumption that we can make on x.

Proposition 5.2.4. *Let $n \geq 12$ and let G and M be as in Notation 5.2.1. Then M is a maximal coclique of $\Gamma(G)$ if and only if for all $x \in G \backslash M$ such that $1^x = k+1$ there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. Since $x \notin M$ there exists $\alpha \in \Omega_1$ and $\beta \in \Omega_2$ such that $\alpha^x = \beta$. If $n - k = 1$, then $\beta = k+1$ and by Lemma 4.1.7 there exists $m \in M$ such that $\alpha^m = 1$. If $n - k \geq 2$, then by Lemma 4.1.7 there exists $m \in M$ such that $\alpha^m = 1$ and $\beta^m = k+1$. By Lemma 5.2.2 it suffices to consider x up to conjugation by M, and so the result follows. □

We now define two distinct hypotheses which between them cover all possibilities in the case where $x \in G \backslash M$ is not a transposition and $n \geq 12$.

Hypothesis 5.2.5. *Let $n \geq 12$ so that $k \geq 7$.*

(A) *Let $G = \mathrm{A}_n$ if n is odd and $G = \mathrm{S}_n$ if n is even.*

(B) *Let $G = \mathrm{A}_n$ if n is even and $G = \mathrm{S}_n$ if n is odd.*

In both cases, assume that $1^x = k+1$ and that $x \neq (1, k+1)$.

For the remainder of the chapter we introduce the following notation, which makes it immediately clear how the cycles of an element of M split across Ω_1 and Ω_2.

Notation 5.2.6. For $y \in M$ define

$$\mathcal{C}_M(y) := \mathcal{C}_1(y) \mid \mathcal{C}_2(y),$$

where $\mathcal{C}_i(y) := \mathcal{C}(y\mid_{\Omega_i})$ for $i = 1, 2$.

Recall by Notation 4.2.2, that for $y \in \mathrm{S}_n$ with disjoint cycle decomposition $c_1 \cdots c_t$, we let $\Theta_i = \mathrm{Supp}(c_i)$ for $1 \leq i \leq t$.

5.3 Proof of Theorems 5.1.1 and 5.1.2

In this section we complete the proofs of Theorems 5.1.1 and 5.1.2. Let G, M, n and x be as in Hypothesis 5.2.5(A) or (B). Using the results of Sections 4.2, 4.3 and 4.4, we construct $y \in M$ such that $H := \langle x, y\rangle$ is primitive and contains a Jordan element. Hence $\mathrm{A}_n \leq H$, and by the parity of y it will follows that $H = G$.

5.3.1 Hypothesis 5.2.5(A)

We begin by putting restrictions on x.

Lemma 5.3.1. *Let n, G, M and x be as in Hypothesis 5.2.5*(A)*. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ and x is a Jordan element, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Hypothesis 5.2.5 $|\mathrm{Supp}(x)| > 2$, and so there exists a point $\alpha \in \mathrm{Supp}(x)\backslash\{1, k+1\}$. Our assumption that $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ implies that $\alpha \in \Omega_2$.

By Lemma 4.2.1, elements of S_n composed of three cycles lie in A_n if and only if $G = \mathrm{A}_n$. Therefore there exists $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k-1) \cdot 1,$$

and $\Theta_3 = \{\alpha\}$. Let $H = \langle x, y\rangle$ and let $Y = \langle y\rangle$. Since $1 \in \Theta_1$ and $k+1 \in \Theta_2$, it follows that $\Theta_1 \cup \Theta_2 = \Omega\backslash\{\alpha\} \subseteq 1^H$. Since $\alpha \in \mathrm{Supp}(x)$, the group H is transitive.

We show that H is primitive. Let Δ be a non-singleton block for H containing α. Let $\beta \in \Delta\backslash\{\alpha\}$. Since α is fixed by y, it follows that $\Delta^y = \Delta$. Hence $\beta^Y \cup \{\alpha\} \subseteq \Delta$. If $\beta \in \Theta_1$, then $\beta^Y \cup \{\alpha\} = \Theta_1 \cup \alpha \subseteq \Delta$. Hence $|\Delta| \geq k+1 > \frac{n}{2}$ and so $\Delta = \Omega$ by Lemma 4.2.6. If $\beta \in \Theta_2$, then $\Theta_2 \cup \{\alpha\} \subseteq \Delta$. Since $\mathrm{Supp}(x) \cap \Theta_1 = \{1\}$ and $(k+1)^{x^{-1}} = 1 \neq \alpha^{x^{-1}}$, it follows that $\alpha^{x^{-1}} \in \Theta_2 \subseteq \Delta$. Hence $\Delta^{x^{-1}} = \Delta$, and so $\Delta^H = \Delta$. By the transitivity of H, it follows that $\Delta = \Omega$.

Hence $H = \langle x, y \rangle$ is primitive, and contains the Jordan element x. Thus $\mathrm{A}_n \leq H$, by Theorem 4.3.4, and so $H = G$ by the parity of y. □

We now show that if $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.

Lemma 5.3.2. *Let n, G, M and x be as in Hypothesis 5.2.5*(A). *If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. We begin by showing that we can make assumptions on x. By Lemma 5.3.1 the result holds if x is a Jordan element, and so by Lemma 8.2.3 the result holds if $n - k \leq 10$. Hence assume otherwise. Therefore $x \notin \mathcal{J}_s$, and so $2(\sqrt{n} - 1) < |\mathrm{Supp}(x)|$. Since $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ it follows that $|\mathrm{Supp}(x)| \leq n - k + 1$. Thus $n - k > 10$ and $2(\sqrt{n} - 1) < n - k + 1$, and so by Lemma 4.4.6 there exists a prime $p^{(2)}$ such that $2 < p^{(2)} < n - k - 3$ and $p^{(2)} \nmid k$. In addition, by Lemma 8.2.2 the result holds if $|\mathrm{Supp}(x)| < 8$ or if $\mathcal{C}(x) = 1^{(n-8)} \cdot 2^4$, so we may assume otherwise. Therefore by Lemma 4.2.3(ii) there exist $\alpha, \alpha^x, \beta, \beta^x, \delta, \epsilon \in \mathrm{Supp}(x) \backslash \{1, k+1\}$ such that (δ, ϵ) is not a cycle of x.

The proof splits into two cases. For each we give an element $y \in M$ such that $H = \langle x, y \rangle$ is transitive and contains an element of $\mathcal{J}_c$. We then prove simultaneously that in both cases H is primitive. First suppose that $p^{(2)} \mid (n-k)$. By Lemma 4.2.1, elements composed of five cycles lie in A_n if and only if $G = \mathrm{A}_n$. Hence there exists $y = c_1c_2c_3c_4c_5 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)} \cdot (n - k - p^{(2)} - 2) \cdot 1 \cdot 1,$$

with $\alpha, \beta, \beta^x \in \Theta_2$, $k+1, \alpha^x \in \Theta_3$, $\Theta_4 = \{\delta\}$ and $\Theta_5 = \{\epsilon\}$. Let $H = \langle x, y \rangle$. Since $1 \in \Theta_1$ and $k + 1 \in \Theta_3$, it follows that $\Theta_1, \Theta_3 \subseteq 1^H$. Then because $\alpha \in \Theta_2$ and $\alpha^x \in \Theta_3$, it follows that $\Theta_2 \subseteq 1^H$. Since (δ, ϵ) is not a cycle of x and $\Omega \backslash \{\delta, \epsilon\} \subseteq 1^H$, the group H is transitive. Since $p^{(2)} > 2$ and $p^{(2)} \mid (n - k)$, it follows that $p^{(2)} \nmid |\Theta_3|$. Hence $y^{k(n-k-p^{(2)}-2)}$ is a $p^{(2)}$-cycle, and so $y^{k(n-k-p^{(2)}-2)} \in \mathcal{J}_c$.

Next suppose that $p^{(2)} \nmid (n - k)$. By Lemma 4.2.1, elements composed of three cycles lie in A_n if and only if $G = \mathrm{A}_n$. Hence there exists $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)} \cdot (n - k - p^{(2)}),$$

with $\alpha, \beta, \beta^x \in \Theta_2$ and $k + 1, \alpha^x \in \Theta_3$. Let $H = \langle x, y \rangle$. Since $1 \in \Theta_1$ and $k + 1 \in \Theta_3$ it follows that $\Theta_1, \Theta_3 \in 1^H$. Finally, from $\alpha \in \Theta_2$ and $\alpha^x \in \Theta_3$, it follows that H is transitive. Since $p^{(2)} \nmid (n-k)$ it follows that $p^{(2)} \nmid |\Theta_3|$. Hence $y^{k(n-k-p^{(2)})}$ is a $p^{(2)}$-cycle, and so $y^{k(n-k-p^{(2)})} \in \mathcal{J}_c$.

Let H be as in either case above and let $\mathcal{H}$ be a non-singleton block system for H. From $p^{(2)} \nmid |\Theta_i|$ for $i \neq 2$, Lemma 4.2.12 implies that there exists a block $\Delta \in \mathcal{H}$ such that $\Theta_2 \subseteq \Delta$. Therefore $\Delta^y = \Delta$. Furthermore, from $\beta, \beta^x \in \Theta_2$ we deduce that $\Delta^H = \Delta$. Hence $\Delta = \Omega$ by the transitivity of H. Thus H is primitive and contains an element of $\mathcal{J}_c$. Therefore $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and by the parity of y it follows that $H = G$. □

We now complete the proof that under Hypothesis 5.2.5(A) there exists $y \in M$ such that $\langle x, y\rangle = G$.

Lemma 5.3.3. *Let n, G, M and x be as in Hypothesis 5.2.5*(A)*. Then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then the result holds by Lemma 5.3.2. Therefore we may assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, and so there exists $\alpha \in \big(\Omega_1 \cap \mathrm{Supp}(x)\big)\backslash\{1\}$. Since $k \geq 7$, there exists a prime p_k such that $5 \leq p_k \leq k-2$, by Theorem 4.4.1.

First assume that $k = p_k + 2$ and $n - k = p_k$. Hence $n = 2p_k + 2$. Thus n is even, and so by Hypothesis 5.2.5(A) it follows that $G = \mathrm{S}_n$. By Lemma 4.2.1, elements of S_n composed of three cycles are in $\mathrm{S}_n\backslash\mathrm{A}_n$. Let $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}_M(y) = 3 \cdot (p_k - 1) \mid p_k,$$

with $1 \in \Theta_1$, $\alpha \in \Theta_2$ and $\alpha^x \notin \Theta_2$. Let $H = \langle x, y\rangle$. Since $1^x = k+1$, it follows that $\Theta_1, \Theta_3 \subseteq 1^H$. Then $\alpha \in \Theta_2$ and $\alpha^x \in \Theta_1 \cup \Theta_3$, so H is transitive.

Let $\mathcal{H}$ be a non-singleton block system for H. Since $p_k \nmid |\Theta_1|, |\Theta_2|$, Lemma 4.2.12 implies that there exists a block $\Delta \in \mathcal{H}$ such that $\Theta_3 \subseteq \Delta$. Hence $\Delta^y = \Delta$, and so Δ is a union of the orbits of y and contains Θ_3. Hence $|\Delta| = p_k, p_k + 3, 2p_k - 1$ or $2p_k + 2$. Since $|\Delta|$ divides $n = 2p_k + 2$, it follows that $|\Delta| = 2p_k + 2$. Hence H is primitive and contains $y^{3(p_k-1)} \in \mathcal{J}_c$. Therefore $H = G$ by Theorem 4.3.4.

Hence for the remainder of the proof we may assume that either $k \neq p_k + 2$ or $n - k \neq p_k$. Since $k - 2 \geq p_k$, it follows that we can assume either

$$k - p_k > 2 \quad \text{or} \quad n - k \neq p_k. \tag{5.1}$$

By Lemma 4.2.1 elements of S_n composed of three cycles are in A_n if and only if $G = \mathrm{A}_n$.

Hence let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}_M(y) = (k - p_k) \cdot p_k \mid (n - k),$$

with $1 \in \Theta_1$, $\alpha \in \Theta_2$ and $\alpha^x \notin \Theta_2$. By Lemma 4.2.1, $\mathcal{Y} \neq \emptyset$, and consists of elements of A_n if and only if $G = \mathrm{S}_n$. For all $y \in \mathcal{Y}$, let $H = H(y) = \langle x, y\rangle$ and let $Y = \langle y \rangle$. The proof of transitivity is identical to the previous case. We assume, by way of contradiction, that $H(y)$ is imprimitive for all $y \in \mathcal{Y}$, and let $\mathcal{H}$ be a non-trivial block system for H.

First suppose, for a contradiction, that there exists $\Delta_1 \in \mathcal{H}$ such that $\Theta_2 \subseteq \Delta_1$. We begin by showing that if $\Theta_2 \subseteq \Delta_1$, then $\Delta_1 = \Theta_2$. Suppose otherwise, and let $\beta \in \Delta_1 \backslash \Theta_2$. From $\Theta_2 \subseteq \Delta_1$ we see that $\Delta_1^y = \Delta_1$. If $\beta \in \Theta_1$, then $\Theta_1 \cup \Theta_2 \subseteq \Delta_1$ and so $|\Delta_1| \geq k > \frac{n}{2}$, a contradiction. Hence $\beta \in \Theta_3$, so $\Theta_2 \cup \Theta_3 \subseteq \Delta_1$, yielding the contradiction

$$|\Delta_1| \geq |\Theta_2| + |\Theta_3| = p_k + n - k > \frac{k}{2} + n - k = n - \frac{k}{2} > \frac{n}{2}.$$

Hence if $\Theta_2 \subseteq \Delta_1$ then $\Delta_1 = \Theta_2$. Therefore $|\Delta_1| = p_k$ and so $p_k \mid n$. Since $\frac{n}{2} < k < 2p_k$, it follows that $n < 4p_k$, and consequently either $n = 2p_k$ or $n = 3p_k$.

If $n = 2p_k$, then $\mathcal{H}$ consists of two blocks $\Delta_1 = \Theta_2$ and $\Delta_2 = \Omega\backslash\Delta_1 = \Theta_1 \cup \Theta_3$. Hence $\{1, k+1\} = \{1, 1^x\} \subseteq \Delta_2$, and so both x and y leave Δ_2 invariant, contradicting the transitivity of H.

If $n = 3p_k$, then there exist blocks Δ_2 and Δ_3 such that $\mathcal{H} = \{\Delta_1, \Delta_2, \Delta_3\}$. Hence $\Delta_2 \cup \Delta_3 = \Theta_1 \cup \Theta_3$. Since $p_k \neq k - p_k$ it follows that Θ_1 is not a block. Therefore Δ_2 and Δ_3 contain points of Θ_1 and Θ_3. Hence $y^{\mathcal{H}} = (\Delta_2, \Delta_3)$. If there exists $\beta \in \Delta_1$ such that $\beta^x \in \Delta_1$, then $\Delta_1^x = \Delta_1 = \Delta_1^y$, a contradiction. Therefore $\Delta_1^x \subseteq \Theta_1 \cup \Theta_3$, and since $|\Delta_1| = p_k \geq 5$, there exist distinct points $\beta, \gamma \in \Delta_1$ such that β^x, γ^x are either both contained in Θ_1 or in Θ_3. Let

$$\mathcal{Y}_1 = \{y \in \mathcal{Y} \mid (\beta^x)^y = \gamma\},$$

and notice that $\mathcal{Y}_1 \neq \emptyset$. Hence for all $y \in \mathcal{Y}_1$, the block Δ_2 contains exactly one of $\{\beta^x, \gamma^x\}$. Thus $\Delta_1^x \cap \Delta_2 \neq \emptyset$ and $\Delta_1^x \neq \Delta_2$, a contradiction.

Therefore if n is even and $y \in \mathcal{Y}$ or if n is odd and $y \in \mathcal{Y}_1$, then there is no block $\Delta_1 \in \mathcal{H}$ satisfying $\Theta_2 \subseteq \Delta_1$. Hence it follows from Lemma 4.2.11(ii) that $c_2^{\mathcal{H}}$ is a p_k-cycle. Let $\Delta \in \mathrm{Supp}(c_2^{\mathcal{H}})$. From $p_k > k - p_k$ it follows that $\Delta \cap \Theta_1 = \emptyset$ by Lemma 4.2.11(iv). Since Δ is non-trivial it follows that $\Delta \cap \Theta_3 \neq \emptyset$. From $|\Delta| > 1$ we deduce that $\Delta \cap \Theta_3 \neq \emptyset$. Hence $c_2^{\mathcal{H}} = c_3^{\mathcal{H}}$ by Lemma 4.2.11(i), and so $p_k \mid (n-k)$ by Lemma 4.2.10. Therefore $p_k = n - k$ by Lemma 4.4.3, and so $|\Delta| = 2$. If n is odd then we reach a contradiction, and so if $y \in \mathcal{Y}_1$, then $H = \langle x, y\rangle$ is primitive. Therefore assume that n is even.

From $\Delta \cap \Theta_1 = \emptyset$, it follows that $c_1^{\mathcal{H}}$ and $c_2^{\mathcal{H}} = c_3^{\mathcal{H}}$ act on disjoint sets of blocks. From $p_k = n - k$ it follows by (5.1) that $|\Theta_1| = k - p_k > 2$. Thus Θ_1 is a union of blocks at least two, $|\Theta_1| \geq 4$ and $c_1^{\mathcal{H}}$ is a cycle of length $\frac{k-p_k}{2}$. Hence there exists $\beta \in \Theta_1 \backslash \{1, \alpha^{x^{-1}}\}$, and the set

$$\mathcal{Y}_\beta = \left\{ y \in \mathcal{Y} \ : \ 1^{y^{\frac{k-p_k}{2}}} = \beta \right\}$$

is non-empty. Hence for all $y \in \mathcal{Y}_\beta$, it follows that $\Gamma = \{1, \beta\}$ is a block for $H(y)$. Consider $\Gamma^x = \{k+1, \beta^x\}$. If $\beta^x \in \Omega_2$, then $\Gamma^x \subseteq \Omega_2 = \Theta_3$, contradicting the fact that $c_3^{\mathcal{H}}$ is a p_k-cycle and so acts regularly on blocks. Hence $\beta^x \in \Omega_1$. Since $\beta \neq \alpha^{x^{-1}}$, it follows that $\beta^x \neq \alpha$. Since $|\Theta_1| \geq 4$, there exists $y \in \mathcal{Y}_\beta$ such that $\beta^x \in \Theta_1$. Thus $k+1 \in \Gamma^x \cap \Theta_3$ and $\beta^x \in \Gamma^x \cap \Theta_1$, contradicting the fact that c_1 and c_3 act on disjoint sets of blocks.

Hence when n is odd there exists $y \in \mathcal{Y}_1$, and when n is even there exists $y \in \mathcal{Y}_\beta$ such that $H = \langle x, y \rangle$ is primitive. If $n - k \neq p_k$, then $y^{(k-p_k)(n-k)}$ is a p_k-cycle; and if $n - k = p_k$, then y^{p_k} is a $(k - p_k)$-cycle. Thus in both cases H contains an element of $\mathcal{J}_c$ and so $H = G$ by Theorem 4.3.4. □

5.3.2 Hypothesis 5.2.5(B)

In this section we show that for n, G, M and x as in Hypothesis 5.2.5(B) there exists $y \in M$ such that $\langle x, y \rangle = G$. This parity proves to be more difficult than the previous and so will require more cases.

We begin with the case $|\Omega_1 \cap \mathrm{Supp}(x)| = 2 = |\Omega_2 \cap \mathrm{Supp}(x)|$.

Lemma 5.3.4. *Let G, M, n and x be as in Hypothesis 5.2.5*(B)*. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 2$ and $|\mathrm{Supp}(x) \cap \Omega_2| = 2$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Let $\Omega_1 \cap \mathrm{Supp}(x) = \{1, \alpha\}$ and $\Omega_2 \cap \mathrm{Supp}(x) = \{k+1, \beta\}$. Then there are three possibilities for x, namely $(1, k+1, \alpha, \beta), (1, k+1, \beta, \alpha)$ or $(1, k+1)(\alpha, \beta)$.

By Lemma 4.2.1, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$. Hence there exists $y = c_1 c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k),$$

with $1^{y^2} = \alpha$ and $(k+1)^y = \beta$. Since $1^x = k+1$, it follows that $H = \langle x, y \rangle$ is transitive.

We prove that H is primitive. Let Δ be a non-singleton block for H containing 1. We shall show that there exists $\gamma \in (\Delta \cap \Theta_1) \backslash \{1\}$. Let $\delta \in \Delta \backslash \{1\}$. If $\delta \in \Theta_1$, then let $\gamma := \delta$. If $\delta \in \Theta_2$, then let $\gamma := 1^{y^{(n-k)}}$. Since $k > n - k$, it follows that $\gamma \neq 1$. From $\delta^{y^{(n-k)}} = \delta$ we deduce that $\Delta^{y^{(n-k)}} = \Delta$, hence $\gamma \in \Delta \cap \Theta_1$.

We claim that $\Delta^x = \Delta$ and so $k + 1 \in \Delta$. If $\gamma \in \mathrm{Fix}(x)$, then this is immediate. If

$\gamma \notin \mathrm{Fix}(x)$, then by looking at $\mathrm{Supp}(x)$ we deduce that $\gamma = \alpha = 1^{y^2}$. Hence $\Delta^{y^2} = \Delta$ and so $1^{y^4} \in \Delta$. Since $k \geq 7$, it follows that $1^{y^4} \neq 1, \alpha$. Hence $1^{y^4} \in \mathrm{Fix}(x)$ and so $\Delta^x = \Delta$.

The block Δ^y contains $\beta = (k+1)^y \in \mathrm{Supp}(x)$ and $\epsilon := 1^y \in \mathrm{Fix}(x)$. Therefore $(\Delta^y)^x = \Delta^y$, and so $\beta^x \in \Delta^y$. By consulting the possibilities for x it is immediate that either $\beta^x = \alpha = \epsilon^y$ or $\beta^x = 1 = \epsilon^{y^{-1}}$. Hence either $\{\epsilon, \epsilon^y\}$ or $\{\epsilon, \epsilon^{y^{-1}}\} \subseteq \Delta^y$. Thus $(\Delta^y)^y = \Delta^y$, and so $\Delta^y = \Delta$. Hence $\Delta^x = \Delta = \Delta^y$, and so $\Delta = \Omega$.

Therefore $H = \langle x, y\rangle$ is primitive. Since $|\mathrm{Supp}(x)| = 4 \leq 2(\sqrt{n} - 1)$ it follows that $x \in \mathcal{J}_s$. Therefore $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and the parity of y implies that $H = G$. □

We now generalise to the case where both $|\Omega_1 \cap \mathrm{Supp}(x)|$ and $|\Omega_2 \cap \mathrm{Supp}(x)|$ are at least 2.

Lemma 5.3.5. *Let n, G, M and x be as in Hypothesis 5.2.5*(B)*. If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \geq 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Lemma 5.3.4, the result holds when $|\mathrm{Supp}(x)| = 4$, and so we may assume that $|\mathrm{Supp}(x)| > 4$. Hence there exist points $\alpha \in \Omega_1\backslash\{1\}$ and $\beta \in \Omega_2\backslash\{k+1\}$ such that $\alpha^x \neq \beta$.

We define $\mathcal{Y}$, a set of elements of M composed of four cycles (with unspecified lengths). We show that for all $y \in \mathcal{Y}$ that $H = \langle x, y\rangle$ is transitive. We then define subsets of $\mathcal{Y}$ based on the lengths of the cycles, and in each case show that H is primitive and contains a Jordan element.

Let $\mathcal{Y}$ be the set of $y = c_1c_2c_3c_4 \in M$ such that $\Theta_1 \cup \Theta_2 = \Omega_1$, $\Theta_3 \cup \Theta_4 = \Omega_2$, $1 \in \Theta_1, \alpha \in \Theta_2$, $\alpha^x \notin \Theta_2$, $k+1 \in \Theta_3$ and $\Theta_4 = \{\beta\}$. By Lemma 4.2.1, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so $\mathcal{Y} \neq \emptyset$. For all $y \in \mathcal{Y}$, let $H = H(y) = \langle x, y\rangle$ and let $Y = \langle y\rangle$.

From $1^x = k+1$ we deduce that $\Theta_1, \Theta_3 \subseteq 1^H$. Since $\alpha^x \neq \beta$ and $\alpha^x \notin \Theta_2$, it follows that $\alpha \in \Theta_1 \cup \Theta_3$. Hence $\Omega\backslash\{\beta\} = \Theta_1 \cup \Theta_2 \cup \Theta_3 \subseteq 1^H$, and since $\beta \in \mathrm{Supp}(x)$, it follows that H is transitive. Assume, by way of contradiction, that H is imprimitive, and let $\mathcal{H}$ be a non-trivial block system for H.

Let p_k be as in Theorem 4.4.1 so that $\frac{k}{2} < p_k < k-1$. We split into two cases. First assume that $p_k = n-k-1$ and $p_k = k - p_k + 1$. Then

$$n = p_k + k + 1 = p_k + 2p_k = 3p_k,$$

and so it follows from Hypothesis 5.2.5(B) that $G = \mathrm{S}_n$. Let

$$\mathcal{Y}_1 = \Big\{ y \in \mathcal{Y} \ : \ \mathcal{C}_M(y) = (p_k + 1) \cdot (p_k - 2) \mid p_k \cdot 1 \Big\}.$$

Then $\mathcal{Y}_1 \neq \emptyset$ and $p_k \nmid |\Theta_1|, |\Theta_2|, |\Theta_4|$. Hence Lemma 4.2.12 implies that there exists a block $\Delta \in \mathcal{H}$ such that $\Theta_3 \subseteq \Delta$, and so $|\Delta| \geq p_k$. Since $n = 3p_k$ and $|\Delta| \mid n$, it follows that $|\Delta| = p_k$ and $\Delta = \Theta_3$. Let Γ be the block containing β. Then $\Gamma^y = \Gamma$, and so Γ is a union of some of the Θ_i. Since $|\Gamma| = p_k$ we reach a contradiction. Therefore for all $y \in \mathcal{Y}_1$, the group $H = \langle x, y \rangle$ is primitive. Furthermore, $y^{(p_k+1)(p_k-2)} \in \mathcal{J}_c$ and so $H = G$ by Theorem 4.3.4.

We may now assume that either

$$p_k \neq k - p_k + 1 \quad \text{or} \quad p_k \neq n - k - 1. \tag{5.2}$$

Let

$$\mathcal{Y}_2 = \Big\{ y \in \mathcal{Y} : \mathcal{C}_M(y) = (k - p_k) \cdot p_k \mid (n - k - 1) \cdot 1 \Big\}.$$

Then $\mathcal{Y}_2 \neq \emptyset$.

We first claim that there exists $\Delta \in \mathcal{H}$ such that $\Theta_2 \subseteq \Delta$. If $p_k \neq n - k - 1$, then $p_k \nmid (n - k - 1)$ by Lemma 4.4.3. In which case $p_k \nmid |\Theta_1|, |\Theta_3|, |\Theta_4|$ and so the claim holds by Lemma 4.2.12. Suppose instead that $p_k = n - k - 1$. If the claim does not hold, then $l(c_2^{\mathcal{H}}) = p_k$ by Lemma 4.2.11(ii). Hence $c_1^{\mathcal{H}}$ and $c_2^{\mathcal{H}}$ act on distinct sets of blocks by Lemma 4.2.11(iv). Since $\mathcal{H}$ is non-trivial it follows that $c_2^{\mathcal{H}} = c_3^{\mathcal{H}}$, and so block size is two. Let $\Gamma \in \mathcal{H}$ be the block which contains β. Then $\Gamma^y = \Gamma$ since β is fixed by y. Hence $\Gamma \notin \mathrm{Supp}(c_2^{\mathcal{H}}) = \mathrm{Supp}(c_3^{\mathcal{H}})$, and so $\Gamma \cap \Theta_1 \neq \emptyset$. Therefore $\Theta_1 \subseteq \Gamma$ and $|\Gamma| \geq k - p_k + 1 > k - (k-1) + 1 = 2$, a contradiction. Hence the claim holds.

We show next that $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$. From $\Theta_2 \subseteq \Delta$ it follows that $|\Delta| \geq p_k > \frac{k}{2} > \frac{n}{4}$, and so $|\mathcal{H}| = 2$ or 3. First suppose that $|\mathcal{H}| = 2$, for which we derive a contradiction. Let $\Gamma = \Omega \backslash \Delta$. Since $\Delta^y = \Delta$, it follows that $\Gamma^y = \Gamma$. If $\Theta_1 \subseteq \Delta$, then

$$|\Delta| \geq (k - p_k) + p_k = k > \frac{n}{2},$$

a contradiction.We now show that $\Theta_3 \not\subseteq \Delta$. Recall that $p_k > \frac{k}{2}$, and so $p_k - k > -\frac{k}{2}$; also by assumption
$n - k = |\Omega_2| \geq 2$ and so $-1 \geq -\frac{n-k}{2}$. Hence if $\Theta_3 \subseteq \Delta$ then

$$|\Delta| \geq p_k + n - k - 1 = n + (p_k - k) - 1 > n - \frac{k}{2} - \frac{n-k}{2} = \frac{n}{2},$$

a contradiction. Therefore $\Theta_1, \Theta_3 \not\subseteq \Delta$ and so $\Theta_1, \Theta_3 \subseteq \Gamma$. Thus $1, k+1 \in \Gamma$ and so $\Gamma^H =$

Γ, a contradiction. Hence $|\mathcal{H}| \neq 2$, and we conclude that $|\mathcal{H}| = 3$. Recall that $\Theta_2 \subseteq \Delta$, and so if $\Delta \cap \Theta_1 \neq \emptyset$ then $\Theta_1 \cup \Theta_2 \subseteq \Delta$. In which case $|\Delta| > \frac{n}{2}$, a contradiction. Hence there exists a block $\Gamma \in \mathcal{H}\backslash\{\Delta\}$ containing a point of Θ_1. If $\Gamma \cap \Theta_3 \neq \emptyset$, then $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$ by Lemma 4.2.11(i), as required. Hence assume for a contradiction that $\Gamma \cap \Theta_3 = \emptyset$, and so $\Theta_2 \subseteq \Delta$ and $\Gamma \subseteq \Theta_1 \cup \Theta_4$. Since $|\Theta_1| < |\Theta_2| \leq |\Delta|$, it follows that $\Theta_4 = \{\beta\} \subseteq \Gamma$. Hence $\Gamma^y = \Gamma$ and $\Gamma = \Theta_1 \cup \{\beta\}$. Therefore the third block of $\mathcal{H}$, say Σ, must contain a point of Θ_3. Since $\Delta^y = \Delta$ and $\Gamma^y = \Gamma$ it follows that $\Sigma^y = \Sigma$. Thus $\Delta = \Theta_2$, $\Gamma = \Theta_1 \cup \{\beta\}$ and $\Sigma = \Theta_3$. Hence $|\Delta| = |\Gamma| = |\Sigma|$ implies that $p_k = k - p_k + 1 = n - k - 1$, contradicting (5.2).

Therefore we have shown that $\Theta_2 \subseteq \Delta$ and so $\Delta^y = \Delta$, and that $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$. If there exists $\delta \in \Delta$ such that $\delta^x \in \Delta$, then $\Delta^H = \Delta$, a contradiction. Hence $\Theta_2^x \subseteq \Theta_1 \cup \Theta_3 \cup \{\beta\}$. By Theorem 4.4.1 $|\Theta_2| = p_k > 5$, and so there exist $\epsilon, \zeta \in \Theta_2$ such that either ϵ^x, ζ^x are both in Θ_1 or both in Θ_3. There exists $y \in \mathcal{Y}_2$ such that $(\epsilon^x)^y = \zeta^x$. Hence $(\Delta^x)^y = \Delta^x$, and so $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$ implies that $\Theta_1 \cup \Theta_3 \subseteq \Delta^x$. In particular, Δ^x contains 1 and $k+1$, and so $(\Delta^x)^x = \Delta^x$. Hence $(\Delta^x)^H = \Delta$, a contradiction.

Therefore for this y the group $H = \langle x, y \rangle$ is primitive. If $p_k \neq n - k - 1$, then $y^{(k-p_k)(n-k-1)}$ is a p_k-cycle. If $p_k = n - k - 1$, then y^{p_k} is a $(k - p_k)$-cycle. Hence H contains an element of $\mathcal{J}_c$. Thus $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

We have reduced to the case of either $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ or $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. We first consider the case where $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$.

Lemma 5.3.6. *Let n, G, M and x be as in Hypothesis 5.2.5*(B). *If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. First assume that x is a Jordan element. It is immediate from Hypothesis 5.2.5 that there exists $\alpha \in \mathrm{Supp}(x)\backslash\{1, k+1\}$, and so $\alpha \in \Omega_2$. Let $\beta := \alpha^{x^{-1}}$. Observe in the following that we only define $k+1, (k+1)^y, (k+1)^{y^2}$ to be distinct when $|\Omega_2 \cap \mathrm{Supp}(x)| \geq 3$. By Lemma 4.2.1, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1 c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k),$$

with $(k+1)^y = \alpha$, and if $\beta \neq k+1$, then $\alpha^y = (k+1)^{y^2} = \beta$. Hence if $\beta = k+1$, then $\beta^y = \alpha$; and otherwise $\alpha^y = \beta$. Let $H = \langle x, y \rangle$. Since $1 \in \Theta_1$ and $k+1 \in \Theta_2$, it follows that H is transitive.

Let $\mathcal{H}$ be a non-singleton block system for H, and let $\Delta \in \mathcal{H}$ with $1 \in \Delta$. We show that there exists $\gamma \in (\Delta \cap \Theta_1)\backslash\{1\}$ (as in Lemma 5.3.4). Since Δ is a non-singleton block there exists $\delta \in \Delta\backslash\{1\}$. If $\delta \in \Theta_1$, then let $\gamma := \delta$. If $\delta \in \Theta_2$, then $\delta^{y^{n-k}} = \delta$, and so $\Delta^{y^{n-k}} = \Delta$. Since $k > n-k$ it follows that $1^{y^{n-k}} \neq 1$, hence $\gamma := 1^{y^{n-k}} \in (\Delta \cap \Theta_1)\backslash\{1\}$. From $\Theta_1 \cap \mathrm{Supp}(x) = \{1\}$ it is immediate that $\gamma \in \mathrm{Fix}(x)$. Hence $\Delta^x = \Delta$, and so $k+1 = 1^x \in \Delta$. Therefore Δ^y contains 1^y and $(k+1)^y = \alpha$. We show that $(\Delta^y)^H = \Delta^y$. Since $1^y \in \Theta_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$, it follows that Δ^y is left invariant by x. Hence $(\Delta^y)^{x^{-1}} = \Delta^y$, and so $\beta = \alpha^{x^{-1}}, \alpha \in \Delta^y$. Either $\alpha^y = \beta$ or $\beta^y = \alpha$ and so $(\Delta^y)^y = \Delta^y$ and $(\Delta^y)^H = \Omega$. Therefore H is primitive. Furthermore, H contains the Jordan element x, so $H = G$.

Hence we may assume that x is not a Jordan element. Therefore in particular $x \notin \mathcal{J}_s$, and so $|\mathrm{Supp}(x)| > 2(\sqrt{n}-1)$. By Lemma 8.2.3, the result holds when $n-k \leq 10$, and so we may assume that $n-k > 10$. Combining these two observations together with Lemma 4.4.6 implies that there exists a prime $p^{(2)}$ such that $2 < p^{(2)} < n-k-3$ and $p^{(2)} \nmid k$. Furthermore, since the result holds when x is a Jordan element, by Lemma 8.2.2 we may assume that $|\mathrm{Supp}(x)| \geq 8$ and $\mathcal{C}(x) \neq 1^{(n-8)} \cdot 2 \cdot 3^2$, $1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-9)} \cdot 3^3$. Hence by Lemma 4.2.3(i) there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x \in \mathrm{Supp}(x)\backslash\{1, k+1\}$. From $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ it follows that $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x \in \Omega_2$.

If $p^{(2)} \nmid (n-k-1)$ then let $i = 1$, otherwise let $i = 2$ so that $p^{(2)} \nmid (n-k-p^{(2)}-i)i$. We now make some observations which will ensure that the placement of points in the elements below are well define. From $p^{(2)} \leq n-k-4$ we see that $n-k-p^{(2)}-i \geq 2$. In addition, since $n-k \geq 11$, it follows that $n-k-i \geq 9$. Hence if $p^{(2)} = 3$, then $n-k-p^{(2)}-i \geq 6$. By Lemma 4.2.1, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)} \cdot (n-k-p^{(2)}-i) \cdot i,$$

with $\alpha, \gamma, \gamma^x \in \Theta_2$, $k+1, \alpha^x \in \Theta_3$, $\beta^x \in \Theta_4$, and if $p^{(2)} \geq 5$ then $\beta \in \Theta_2$, otherwise $\beta \in \Theta_3$. Let $H = \langle x, y\rangle$. It is easy to see that H is transitive.

Let $\mathcal{H}$ be a non-singleton block system for H. From $p^{(2)} \nmid |\Theta_1|, |\Theta_3|, |\Theta_4|$, Lemma 4.2.12 implies that, there exists $\Delta \in \mathcal{H}$ with $\Theta_2 \subseteq \Delta$. Hence $\Delta^y = \Delta$ and $\gamma, \gamma^x \in \Delta$, and so $\Delta^H = \Delta = \Omega$. Thus H is a primitive group containing the $p^{(2)}$-cycle $y^{k(n-k-p^{(2)}-i)i} \in \mathcal{J}_c$. Therefore $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

It remains to consider $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. We first suppose that x is a Jordan element.

Lemma 5.3.7. *Let G, M, n and x be as in Hypothesis 5.2.5*(B)*. If $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ and x is a Jordan element, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. It is immediate from Hypothesis 5.2.5 that there exists $\alpha \in \mathrm{Supp}(x)\backslash\{1, k+1\}$.

Our assumptions that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ and $1^x = k+1$ imply that $\alpha, \alpha^x \in \Omega_1$.

By Lemma 4.2.1, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$. Hence there exists $y = c_1c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k),$$

with $1^y = \alpha$ and if $\alpha^x \neq 1$, then $\alpha^y = \alpha^x$. Hence $\Theta_1 = \Omega_1$ and $\Theta_2 = \Omega_2$. It is clear that $H = \langle x, y \rangle$ is transitive.

We assume, by way of contradiction, that H is imprimitive and let $\mathcal{H}$ be a non-singleton block system for H. Let $\Delta \in \mathcal{H}$ be the block containing $k+1$ and some $\beta \in \Delta \backslash \{k+1\}$. If $n-k=1$, then $\Delta^y = \Delta$ and $\beta \in \Theta_1$. Hence $\beta^{\langle y \rangle} \cup \{k+1\} = \Omega = \Delta$, and so H is primitive. Therefore assume that $n-k \geq 2$.

We claim that $1 \in \Delta$. To see this, let $\Gamma \in \mathcal{H}$ be the block containing 1. If $\Gamma \cap \mathrm{Fix}(x) \neq \emptyset$, then $\Gamma^x = \Gamma$ and so $k+1 = 1^x \in \Gamma$. Hence $\Gamma = \Delta$ and the claim holds. Similarly, if $\Delta \cap \mathrm{Fix}(x) \neq \emptyset$, then $\Delta = \Gamma$. Hence we may assume that $\Delta, \Gamma \subseteq \mathrm{Supp}(x)$. From $|\Theta_2 \cap \mathrm{Supp}(x)| = 1$, it follows that Δ and Γ both contain points of Θ_1. Since Δ contains a point of Θ_2, we deduce that $c_1^{\mathcal{H}} = c_2^{\mathcal{H}}$ by Lemma 4.2.11(i). Hence $\Delta \cap \Theta_2 \neq \emptyset$. Since $\Delta \subseteq \mathrm{Supp}(x)$ and $\Theta_2 \cap \mathrm{Supp}(x) = \{1\}$ it follows that $1 \in \Delta$ and so $\Delta = \Gamma$. Therefore $1, k+1 \in \Delta$.

The block Δ^y contains $1^y = \alpha$ and $(k+1)^y \in \mathrm{Fix}(x)$. Hence $(\Delta^y)^x = \Delta^y$, and so in particular $\{\alpha, \alpha^x\} \subseteq \Delta^y$. If $\alpha^x = 1$, then $\{\alpha, \alpha^x\} = \{1^y, 1\}$; and if $\alpha^x \neq 1$, then $\{\alpha, \alpha^x\} = \{\alpha, \alpha^y\}$. Hence $\Delta^y = (\Delta^y)^H = \Omega$. Therefore H is primitive and contains the Jordan element x, and so $H = G$ by Theorem 4.3.4. □

Finally, we generalise to the case $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$.

Lemma 5.3.8. *Let n, G, M and x be as in Hypothesis 5.2.5*(B)*. If $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If x is a Jordan element, then the result holds by Lemma 5.3.7. If $k \leq 9$ then the result holds by Lemma 8.2.4. Hence we may assume that $k \geq 10$. Then by Lemma 4.4.5 there exists a prime $p^{(1)}$ such that $2 < p^{(1)} \leq k-5$ and $p^{(1)} \nmid (n-k)$. By Lemma 8.2.2 the result holds if $|\mathrm{Supp}(x)| < 8$ or $\mathcal{C}(x) = 1^{(n-8)} \cdot 2 \cdot 3^2$, $1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-9)} \cdot 3^3$. Thus assume otherwise, and so by Lemma 4.2.3(i) there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x \in \mathrm{Supp}(x) \backslash \{1, k+1\}$. Since $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ it follows that $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x \in \Omega_1$.

If $p^{(1)} \nmid (k-1)$, then let $i = 1$, otherwise let $i = 2$. Hence $p^{(1)} \nmid (k - i - p^{(1)})i$. We now make an observation on $k - i - p_k$ which will show that the placement of points in the element below are well defined. Since $p_k \leq k-5$ it follows that $k-p_k \geq 5$ and so $k-p_k-i \geq 3$. By Lemma 4.2.1, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}_M(y) = (k-i-p^{(1)}) \cdot p^{(1)} \cdot i \mid (n-k),$$

with $1, \alpha, \beta \in \Theta_1$, $\alpha^x, \gamma, \gamma^x \in \Theta_2$ and $\beta^x \in \Theta_3$. Let $H = \langle x, y \rangle$. Then it is easy to check that H is transitive.

Let $\mathcal{H}$ be a non-singleton block system for H. Since $p^{(1)} \nmid |\Theta_1||\Theta_2||\Theta_4|$, Lemma 4.2.12 implies that there exists $\Delta \in \mathcal{H}$ such that $\Theta_2 \subseteq \Delta$. Hence $\Delta^y = \Delta$ and $\gamma, \gamma^x \in \Delta$. Therefore $\Delta = \Delta^H = \Omega$, and so H is primitive. Furthermore, H contains the $p^{(1)}$-cycle $y^{(k-i-p^{(1)})i(n-k)} \in \mathcal{J}_c$ and so $H = G$ by Theorem 4.3.4. □

Lemma 5.3.9. *Let n, G, M and x be as in Hypothesis 5.2.5*(B)*. Then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $|\Omega_i \cap \mathrm{Supp}(x)| \geq 2$ for $i \in \{1,2\}$, then result holds by Lemma 5.3.5. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ then the result holds by Lemma 5.3.6, and if $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ then the result holds by Lemma 5.3.8. □

5.3.3 Completing the proof of Theorems 5.1.1 and 5.1.2

If $n \geq 12$ and $x \in G \backslash M$ is not a transposition, then by Lemmas 5.3.3 and 5.3.9 there exists $y \in M$ such that $\langle x, y \rangle = G$. Here we consider the case of $x \in G \backslash M$ a transposition. We then prove Theorems 5.1.1 and 5.1.2.

Theorem 5.3.10. *Let $n, k, G = \mathrm{S}_n$ and M be as in Notation 5.2.1, and let $x \in G \backslash M$ be a transposition. Then there exists $y \in M$ such that $\langle x, y \rangle = G$ if and only if* $\gcd(n,k) = 1$.

Proof. By Proposition 5.2.4, it suffices to consider $x = (1, k+1)$.

First assume that $\gcd(n,k) = 1$. Let $y = c_1c_2 \in M$ such that $\mathcal{C}_M(y) = k \mid (n-k)$, and let $H = \langle x, y \rangle$. Then $1 \in \Theta_1$ and $k+1 \in \Theta_2$, and so H is transitive. Let Δ be a non-singleton block for H containing 1, and let $\alpha \in \Delta \backslash \{1\}$. If $\alpha \in \Omega_1$, then $\alpha^x = \alpha$ and so $\Delta^x = \Delta$. Hence $k+1 = 1^x \in \Delta$. Therefore, without loss of generality, $\alpha \in \Omega_2$. Thus $\alpha^{y^{(n-k)}} = \alpha$, and so $\Delta^{y^{(n-k)}} = \Delta$. Hence $1^{\langle y^{(n-k)} \rangle} \subseteq \Delta$. It follows from $\gcd(n,k) = 1$ that $1^{\langle y^{(n-k)} \rangle} = \Omega_1$. Thus $|\Delta| \geq k+1 > \frac{n}{2}$, so $\Delta = \Omega$ and H is primitive. Since $x \in \mathcal{J}_c$ it follows that $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = \mathrm{S}_n$ since $x \in \mathrm{S}_n \backslash \mathrm{A}_n$.

Next assume that $\gcd(n,k) = t > 1$. Let $y \in M$ be such that $\langle x, y \rangle$ is transitive. Then the only possible cycle structure of y is $\mathcal{C}_M(y) = k \mid (n-k)$. We claim that the set of translates of $\Delta = 1^{\langle y^t \rangle} \cup (k+1)^{\langle y^t \rangle}$ form a proper non-trivial block system for $\langle x, y \rangle$. From which it will follow that $\langle x, y \rangle$ is imprimitive, and so is not equal to S_n. To see this, notice that

$$|\Delta| = |1^{\langle y^t \rangle}| + |(k+1)^{\langle y^t \rangle}| = \frac{k}{t} + \frac{n-k}{t} = \frac{n}{t} > 1.$$

Also, note that $\dot{\bigcup}_{i=0}^{t-1} \Delta^{y^i} = \Omega$ and x fixes Δ^{y^i} setwise for $0 \leq i \leq t-1$. □

By combining the results covered so far we now prove Theorem 5.1.1, which determines when M is a maximal subgroup in $\Gamma(G)$.

Proof of Theorem 5.1.1. let $n \geq 4$, let $\frac{n}{2} < k < n$, let $G = \mathrm{S}_n$ or A_n, and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$. Recall that M is a maximal coclique in $\Gamma(G)$ if and only if for all $x \in G \backslash M$ there exists $y \in M$ such that $\langle x, y \rangle = G$. By Proposition 5.2.4 we may assume without loss of generality that $1^x = k+1$.

If $n \leq 11$, then the result holds by Lemma 5.2.3, so assume that $n \geq 12$. First let $G = \mathrm{S}_n$ and $\gcd(n,k) = 1$, or let $G = \mathrm{A}_n$. Then Lemmas 5.3.3 and 5.3.9 and Theorem 5.3.10 imply that for all $x \in G \backslash M$ there exists $y \in M$ such that $\langle x, y \rangle = G$. Now let $G = \mathrm{S}_n$ and $\gcd(n,k) > 1$. Then by Theorem 5.3.10 $\langle (1, k+1), y \rangle \neq G$ for all $y \in M$. □

We now prove Theorem 5.1.2, in which determines the maximal cocliques for the exceptional cases in Theorem 5.1.1.

Proof of Theorem 5.1.2. Let $2 \leq \frac{n}{2} < k < n$, let $G = \mathrm{S}_n$ or A_n and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$.

In Parts (i)(b), (ii)(a) and (ii)(b) follow immediately from Lemma 5.2.3.

It remains to prove (i)(a). Hence let $G = \mathrm{S}_n$, let $\gcd(n,k) > 1$, and let C be a maximal coclique of $\Gamma(G)$ which contains $M \backslash \{1\}$. Then $C \neq M \backslash \{1\}$ by Theorem 5.1.1. If $x \in G \backslash M$ is not a transposition, then by Lemmas 5.3.3 and 5.3.9 there exists $y \in M$ such that $\langle x, y \rangle = G$. Hence

$$M \backslash \{1\} \subsetneq C \subseteq (M \backslash \{1\}) \cup (1, k+1)^M.$$

Let $z_1, z_2 \in (M \backslash \{1\}) \cup (1, k+1)^M$. If $z_1, z_2 \in M$ then $\langle z_1, z_2 \rangle \leq M \lneq G$. If $z_1 \in M$ and $z_2 \in (1, k+1)^M$ then $\langle z_1, z_2 \rangle \neq G$ by Theorem 5.3.10. If $z_1, z_2 \in (1, k+1)^M$ then $\langle z_1, z_2 \rangle$ is a dihedral group, and since $n \geq 3$ it follows that $\langle z_1, z_2 \rangle \neq G$. Hence $(M \backslash \{1\}) \cup (1, k+1)^M$ is a coclique and so $C = (M \backslash \{1\}) \cup (1, k+1)^M$. □

5.4 Proof of Theorem 5.1.4

Let $p \geq 5$ be a prime such that $p \neq \frac{q^d-1}{q-1}$ for all prime powers q and $d \geq 2$, and let $G = \mathrm{S}_p$ or A_p. In this section we prove Theorem 5.1.4, namely we determine which maximal subgroups of G are maximal cocliques in $\Gamma(G)$.

The methods here are different to those in Section 3, because we can use the following theorem to classify the maximal subgroups of S_p and A_p.

Theorem 5.4.1 ([23, p.99])**.** *A transitive group of prime degree p is one of the following:*

(i) *the symmetric group* S_p *or the alternating group* A_p*;*

(ii) *a subgroup of* $\mathrm{AGL}_1(p)$*;*

(iii) *a permutation representation of* $\mathrm{PSL}_2(11)$ *of degree 11;*

(iv) *one of the Mathieu groups* M_{11} *or* M_{23} *of degree 11 or 23, respectively; or*

(v) *a group* G *with* $\mathrm{PSL}_d(q) \leq G \leq \mathrm{P\Gamma L}_d(q)$ *of degree* $p = \frac{q^d-1}{q-1}$.

We consider M_{23} and $\mathrm{AGL}_1(p)$ separately, and then prove Theorem 5.1.4. We begin with a preliminary lemma which we use in the case of $\mathrm{M}_{23} \leq \mathrm{A}_{23}$.

For a finite group G and a prime p let $\mathrm{Syl}_p(G)$ be the set of all Sylow p-subgroups of G.

Lemma 5.4.2. *Let* $G = \mathrm{A}_{23}$ *and let* $M = \mathrm{M}_{23}$*. Then the following hold.*

(i) *There are two conjugacy classes of subgroups isomorphic to* M *in* G*, which we label* $\mathcal{U}$ *and* $\mathcal{V}$*.*

(ii) *If* K *is a proper transitive subgroup of* G*, then there exists* $W \in \mathcal{U} \cup \mathcal{V}$ *such that* $K \leq W$*.*

(iii) *The Sylow 23-subgroups of* M *are cyclic and transitive.*

(iv) *If* $x \in G \backslash M$ *has order at least 4, then* x *lies in at most 4608 groups of* $\mathcal{U}$ *and at most 4608 groups of* $\mathcal{V}$*.*

(v) *If* $Z \in \mathrm{Syl}_{23}(G)$*, then* Z *lies in exactly one group of* $\mathcal{U}$ *and exactly one group of* $\mathcal{V}$*.*

(vi) *If* $U \in \mathcal{U}$ *and* $V \in \mathcal{V}$ *then* U *and* V *share at most one Sylow 23-subgroup.*

Proof. We prove each part using [33, Code 10] in Magma, we summarise the methods here.

(i) Let G be the largest maximal subgroups of S_{23}, so that $G = \mathrm{A}_{23}$. Then G has thirteen conjugacy classes of maximal subgroups, only two of which are conjugate to M_{23} in S_{23}. Label these two conjugacy classes $\mathcal{U}$ and $\mathcal{V}$.

(ii) The only conjugacy classes of maximal subgroups which are transitive are $\mathcal{U}$ and $\mathcal{V}$. Hence the result follows.

Since $\mathcal{U}$ and $\mathcal{V}$ are conjugate in S_{23} and $G \trianglelefteq \mathrm{S}_{23}$ we may let $M \in \mathcal{U}$ and prove (iii)-(v) for $\mathcal{U}$. The result will then follow for $\mathcal{V}$.

(iii) Since $23 \mid |M|$ and $23^2 \nmid |G|$ it follows that Sylow 23-subgroups of G and M have order 23. Since A_{23} and M_{23} contain a 23-cycles, as an immediate consequence the Sylow 23-subgroups are cyclic and transitive.

(iv) Let $C :=$ ConjugacyClasses(G) and let $P :=$ PermutationCharacter(G, M). Then C is the sequence of conjugacy class representatives of elements of G listed in ascending order, and $P[i]$ is the number of cosets of M in G that are stabilized by $C[i]$. We verify that M is self-normalising in G, and so by Lemma 4.6.2, $P[i]$ is the number of conjugates of M in G containing $C[i]$.

Let $o(C[i])$ denote the order of the element $C[i]$ in G. From $o(C[13]) = 3$ and $o(C[14]) = 4$ it follows that $o(C[i]) \geq 4$ exactly when $i \geq 14$. In addition $P[i] \leq 4608$ for $i \geq 14$. Hence if $g \in G$ has order at least four, then g lies in at most 4068 groups of $\mathcal{U}$.

(v) Using the notation as above $o(C[i]) = 23$ if and only if $i = 276$ or 277. Hence G has two conjugacy classes of element of order 23. Since $P[266] = P[277] = 1$ it follows that elements of order 23 lie in exactly one group of $\mathcal{U}$.

(vi) Let $Z \in \mathrm{Syl}_{23}(G)$. Then by Part (v) there exists exactly one $U \in \mathcal{U}$ and $V \in \mathcal{V}$ such that $Z \leq U \cap V$. Since $\mathrm{N}_U(Z) = \mathrm{N}_G(Z)$ it follows that $\mathrm{N}_U(Z) = \mathrm{N}_V(Z)$. Hence the result follows since $\mathrm{N}_G(Z)$ is a maximal subgroup of U. □

Lemma 5.4.3. *Let $G = \mathrm{A}_{23}$ and $M = \mathrm{M}_{23}$. Then M is a maximal coclique in $\Gamma(G)$.*

Proof. Let $G = \mathrm{A}_{23}$. By Lemma 5.4.2(i), there are two conjugacy classes of M_{23} in G which we call $\mathcal{U}$ and $\mathcal{V}$. Since $\mathcal{U}$ and $\mathcal{V}$ are conjugate in S_{23} and $G \trianglelefteq \mathrm{S}_{23}$, it suffices to show that $M \in \mathcal{U}$ is a maximal coclique in $\Gamma(G)$. Let $x \in G \backslash M$. We show that there exists $y \in M$ such that $\langle x, y\rangle = G$. In certain places we use [33, Code 11] in Magma.

First assume that x has order at least four. Let $Z_1 \in \mathrm{Syl}_{23}(M) \subseteq \mathrm{Syl}_{23}(G)$. Then $[M : \mathrm{N}_M(Z_1)] = 40320$, and so $|\mathrm{Syl}_{23}(M)|$. By Lemma 5.4.2(v) each $Z \in \mathrm{Syl}_{23}(M)$ is contained in exactly one group of $\mathcal{V}$. By Lemma 5.4.2(iv) x lies in at most 4608 groups of $\mathcal{V}$. Hence by Lemma 5.4.2(vi), there are $40320 - 4608 = 35712$ choices of $Z \in \mathrm{Syl}_{23}(M)$ for which $H := \langle x, Z\rangle$ is contained in no group of $\mathcal{V}$. Again by Lemma 5.4.2(v), the only group of $\mathcal{U}$ containing Z is M. Since $x \notin M$ it follows that H is contained in no group of $\mathcal{U}$. By Lemma 5.4.2(iii) Z is transitive and there exists $y \in Z$ such that $Z = \langle y \rangle$. Hence H is transitive and $H = \langle x, y \rangle$. Since H is contained in no group of $\mathcal{U}$ or $\mathcal{V}$, it follows that $H = G$ by Lemma 5.4.2(ii).

Now let x have order two or three, and let $Z \in \mathrm{Syl}_{23}(M)$. Then Z is transitive and there exists $y \in Z$ such that $Z = \langle y \rangle$ by Lemma 5.4.2(iii). By Lemma 5.4.2(v) the only group of $\mathcal{U}$ containing Z is M, and there is exactly one group of $\mathcal{V}$ containing Z, which we call N. If $x \notin N$, then from $x \notin M$ it follows that $H := \langle x, y \rangle$ is contained in no group of $\mathcal{U} \cup \mathcal{V}$. Since H is transitive we deduce by Lemma 5.4.2(ii) that $H = G$.

Therefore assume that $x \in N$ and proceed via Magma. To set up this situation, fix $M \in \mathcal{U}$, $Z \in \mathrm{Syl}_{23}(M)$, $N_0 \in \mathcal{V}$ and $Z_0 \in \mathrm{Syl}_{23}(N_0)$. By Sylow's Theorem there exists $g \in G$ such that $Z_0^g = Z$. Then $N_0^g \in \mathcal{V}$ and $Z \leq N_0^g$, and so $N_0^g = N$ by Lemma 5.4.2(v). Then it can be seen that there are 60467 possibilities for $x \in N \backslash M$ which have order two or three. For each such possible x it can be verified in Magma that there exists $y \in M$ such that $\langle x, y \rangle = G$. □

We now consider $\mathrm{AGL}_1(p)$ as a maximal subgroup of A_p.

Lemma 5.4.4. *Let p be a prime such that $p \neq \frac{q^d-1}{q-1}$, for any prime power q and $d \geq 2$. Let $G = \mathrm{S}_p$, or let $p \neq 11, 23$ and $G = \mathrm{A}_p$. Then $M = \mathrm{AGL}_1(p) \cap G$ is a maximal coclique in $\Gamma(G)$.*

Proof. By Theorem 5.4.1 the only transitive subgroups of S_n are A_n and $\mathrm{AGL}_1(p)$, and the only transitive subgroups of A_n are $\mathrm{AGL}_1(p) \cap \mathrm{A}_n$. Let $x \in G \backslash M$, we show that there exists $y \in M$ such that $\langle x, y \rangle = G$.

First assume either that $G = \mathrm{S}_p$ and $x \in G \backslash M$ is an odd permutation; or that $G = \mathrm{A}_p$. Let $y \in M$ be a p-cycle. Then $H := \langle x, y \rangle$ is transitive. By Lemma 4.6.8(iv), $M = \mathrm{N}_G(\langle y \rangle)$, and so y is contained in no other conjugate of M. Since $x \notin M$ it follows that H is contained in no conjugate of M. Hence $\mathrm{A}_n \leq H$ by Theorem 5.4.1. If $G = \mathrm{A}_p$ then $H = G$ automatically, and if $G = \mathrm{S}_p$ then $x \in \mathrm{S}_p \backslash \mathrm{A}_p$ and so $H = G$.

Therefore for the remainder of the proof we may assume that $G = \mathrm{S}_p$ and $x \in G \backslash M$ is an even permutation. First let x be a p-cycle. By Lemma 4.6.8(iii), there exist $(p-1)$-cycles $y_1, y_2 \in M$ with different fixed points. Therefore $y_1, y_2 \in G \backslash \mathrm{A}_p$ and $\langle y_1 \rangle \neq \langle y_2 \rangle$. Hence $H_1 = \langle x, y_1 \rangle$ and $H_2 = \langle x, y_2 \rangle$ are transitive subgroups of G which are not contained in A_p. Theorem 5.4.1 implies that H_1 and H_2 are either conjugate to M, or equal to G. In the latter case the result follows, and so assume for a contradiction that H_1 and H_2

are both conjugate to M. By Lemma 4.6.8(iv) the unique conjugate of M containing x is $\mathrm{N}_G(\langle x \rangle)$. Hence $H_1 = \mathrm{N}_G(\langle x \rangle) = H_2$, and so $\langle y_1, y_2 \rangle \leq H_1$. By Lemma 4.6.8(v) $M = \langle y_1, y_2 \rangle$ and so $M = H_1$, a contradiction since $x \notin M$.

Assume next that x lies in no conjugate of M and let $\alpha \in \mathrm{Supp}(x)$. By Lemma 4.6.8(iii) there exists a $(p-1)$-cycle $y \in M$ fixing α. Then $\langle x, y \rangle$ is transitive and contained in no conjugate of M. Since $y \notin \mathrm{A}_n$ it follows by Theorem 5.4.1 that $\langle x, y \rangle = G$.

Finally assume that x is an even permutation, not a p-cycle and lies in some conjugate of M. Since x is even it follows that x is not a $(p-1)$-cycle, and so by Lemma 4.6.8(ii) is a proper power of a $(p-1)$-cycle. We claim there exists a $(p-1)$-cycle y in M and $z \in \langle y \rangle$, such that $H = \langle x, y \rangle$ is transitive and $1 < |\mathrm{Fix}(xz^{-1})| < p$. By Lemma 4.6.8(ii) each non-identity element of M has at most one fixed point and so it will follow that H lies in no conjugate of M. Hence $\mathrm{A}_n \leq H$ by Theorem 5.4.1, and since $y \in \mathrm{S}_p \backslash \mathrm{A}_p$ the result will hold.

It remains to prove the claim. Since x is a proper power of a $(p-1)$-cycle, x has one fixed point which we shall call β. Let M_β denote the point stabilizer of β in M. By Lemma 4.6.8(iv) there exist a unique cyclic p-subgroup of M, which we label P.

Since $p \geq 5$, there exist distinct points $\gamma, \delta \in \mathrm{Supp}(x)$. By Lemma 4.6.8(i) M is 2-transitive, and so there exists z_1 in M such that $\gamma^{z_1} = \gamma^x$ and $\delta^{z_1} = \delta^x$. First assume that $z_1 \notin M_\beta \cup P$. Then $z_1 \notin P$ implies that z_1 is neither a p-cycle nor the identity. Thus by Lemma 4.6.8(ii) there exists a $(p-1)$-cycle y such that $z_1 \in \langle y \rangle$. From $z_1 \notin M_\beta$ we deduce that $\beta \in \mathrm{Supp}(z_1) \subseteq \mathrm{Supp}(y)$. Hence $H = \langle x, y \rangle$ is transitive, $\gamma, \delta \in \mathrm{Fix}(xz_1^{-1})$ and $\beta \notin \mathrm{Fix}(xz_1^{-1})$, so the claim follows.

Suppose instead that $z_1 \in M_\beta \cup P$. Since $z_1 \neq x$ there exists $\epsilon \in \mathrm{Supp}(x) \backslash \{\gamma, \delta\}$ such that $\epsilon^{z_1} \neq \epsilon^x$. By Lemma 4.6.8(i), there exists $z_2 \in M$ such that $\gamma^{z_2} = \gamma^x$ and $\epsilon^{z_2} = \epsilon^x$. If $z_2 \notin M_\beta \cup P$, then the result follows as for z_1 with $\gamma, \epsilon \in \mathrm{Fix}(xz_2^{-1})$ and $\beta \notin \mathrm{Fix}(xz_2^{-1})$.

Therefore suppose that $z_1, z_2 \in M_\beta \cup P$. It follows from $\epsilon^{z_1} \neq \epsilon^x = \epsilon^{z_2}$ that $z_1 \neq z_2$. By Lemma 4.6.8(i), M is sharply 2-transitive, and so z_1 is the unique element of M mapping γ to γ^x and δ to δ^x. Hence $\gamma^{z_1} = \gamma^x = \gamma^{z_2}$ and $z_1 \neq z_2$, imply that $\delta^{z_2} \neq \delta^x = \delta^{z_1}$.

Since M is sharply 2-transitive on Ω, it follows that M_β is sharply transitive on $\Omega \backslash \{\beta\}$. Since P is cyclic is follows that P is sharply transitive on Ω. Let Z_1 and Z_2 be the maximal cyclic subgroups of M containing z_1 and z_2. Then z_1 is the unique element of Z_1 sending δ to δ^x, and z_2 is the unique element of Z_2 sending ϵ to ϵ^x. Since $\gamma^{z_1} = \gamma^x = \gamma^{z_2}$ it follows from the sharp transitivity of M_β and P that $\{Z_1, Z_2\} = \{M_\beta, P\}$.

By Lemma 4.6.8(i), there exists $z_3 \in M$ such that $\delta^{z_3} = \delta^x$ and $\epsilon^{z_3} = \epsilon^x$. From $\epsilon^{z_1} \neq \epsilon^x$ and $\delta^{z_2} \neq \delta^x$ we deduce that $z_3 \neq z_1, z_2$. From $\delta^{z_1} = \delta^{z_3}$ and $\epsilon^{z_2} = \epsilon^{z_3}$, the sharp transitivity of M_β and P imply that $z_3 \notin Z_1 \cup Z_2 = M_\beta \cup P$. Therefore there exists a $(p-1)$-cycle $y \in M$ and $t \in \mathbb{N}$ such that $y^t = z_3$. Then y satisfies the claim with $\delta, \epsilon \in \mathrm{Fix}(xy^{-t}) = \mathrm{Fix}(xz_3^{-1})$ and $\beta \notin \mathrm{Fix}(xz_3^{-1})$. Therefore the claim and the theorem follow. □

We can now complete the proof of Theorem 5.1.4.

Proof of Theorem 5.1.4. Let $p \geq 5$ be a prime with $p \neq \frac{q^d-1}{q-1}$ for all prime powers q and $d \geq 2$. Let $G = \mathrm{S}_p$ or A_p and let M be a maximal subgroup of G. If M is intransitive then $M = (\mathrm{S}_k \times \mathrm{S}_{p-k}) \cap G$ for some $\frac{p}{2} < k < p$. Since p is prime it follows that $\gcd(p,k) = 1$, and so the result holds by Theorem 5.1.1. Hence we may assume that M is transitive, and so M is one of the groups in Theorem 5.4.1.

First let $p = \{11, 23\}$ and $G = \mathrm{A}_p$. Since $\mathrm{PSL}_2(11), \mathrm{AGL}_1(11) \cap G \leq \mathrm{M}_{11}$ and $\mathrm{AGL}_1(23) \cap G \leq \mathrm{M}_{23}$, we need only consider the Mathieu groups. If $p = 11$, then [33, Code 12] in Magma, which is similar to the code described in the proof of Lemma 5.2.3, shows that M_{11} is a maximal coclique in $\Gamma(\mathrm{A}_{11})$. By Lemma 5.4.3 M_{23} is a maximal coclique in $\Gamma(\mathrm{A}_{23})$. Hence if $G = \mathrm{A}_p$, then we may assume that $p \neq 11, 23$.

If $G = \mathrm{S}_n$ or A_n and $M = \mathrm{AGL}_1(p) \cap G$, then the result follows by Lemma 5.4.4.

It remains to consider $G = \mathrm{S}_p$, and $M = \mathrm{A}_p$. Let $x \in G \backslash M$, by Lemma 4.6.4 there exists a p-cycle $y \in M$ such that y is not normalized by x. Then $H := \langle x, y \rangle$ is a transitive, and by Lemma 4.6.8(iv) is contained in no conjugate of $\mathrm{AGL}_1(p) \cap G$. Since $x \notin M$ it follows that $H = G$. □

Chapter 6

Imprimitive subgroups as cocliques

Let G be $\mathrm{S}_n := \mathrm{Sym}(\{1,\dots,n\})$ or $\mathrm{A}_n := \mathrm{Alt}(\{1,\dots,n\})$ and let M be an imprimitive maximal subgroup of G. Our main result shows that, when n is suitably large, M is a maximal coclique in the generating graph $\Gamma(G)$ of G. Then under certain restrictions on n, we consider all maximal subgroups of G and determine which are maximal cocliques in $\Gamma(G)$.

Although the results in this section are similar to those in Chapter 5, they seem to require more lengthy and complex proofs. We split into many more cases, use a different approach for proving primitivity and rely more heavily on number theory.

6.1 Introduction

Our main theorem is as follows.

Theorem 6.1.1. *Let $m, k \in \mathbb{N}$ such that $m, k \geq 2$, let $n = mk$, let $G = \mathrm{S}_n$ or A_n, and let $M = \big(\mathrm{S}_k \operatorname{wr} \mathrm{S}_m\big) \cap G$ be an imprimitive maximal subgroup of G. If either $m \geq 27$ or $k \geq 28$, then M is a maximal coclique in $\Gamma(G)$.*

We plan in future to resolve this question for all $n \geq 4$.

Using Theorem 6.1.1 and the results in Chapter 5, we then prove the following.

Theorem 6.1.2. *Let $n \geq 27 \cdot 28 = 756$, let $G = \mathrm{S}_n$ or A_n, and let M be a maximal subgroup of G. If the only proper primitive subgroup of S_n is A_n, then M either is a maximal coclique in $\Gamma(G)$ or $(G, M) = (\mathrm{S}_n, \mathrm{S}_k \times \mathrm{S}_{n-k})$ with $\gcd(n, k) > 1$.*

As context for the density of integers for which the above theorem applies, Cameron, Neumann and Teague prove in [15] that for almost all integers n, the only primitive groups of degree n are the symmetric and alternating groups. The following is an example of such n. If $p \neq 11$ is a prime which is not equal to $\frac{q+1}{2}$ for any prime power q, then by [25, Lemma 1] the only proper primitive subgroup of S_{2p} is A_{2p}.

This chapter is structured as follows. In Section 6.2 we define the notation for the rest of the chapter. In Section 6.3 we prove Theorem 6.1.1 provided the existence of a Jordan element. We then divide the possibilities for m and k into six regions as illustrated in the following diagram.

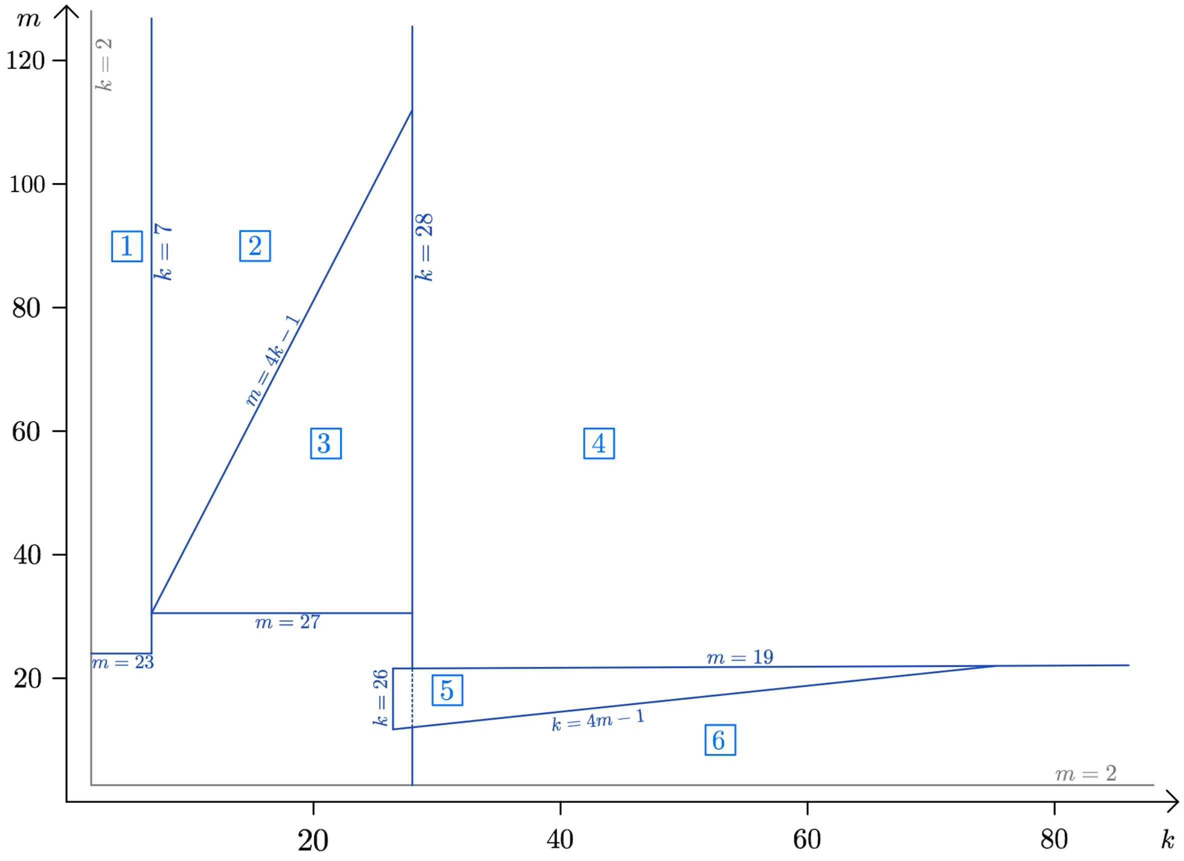


Figure 6.1: Patchwork Proof - Division of m and k into regions.

1. $2 \leq k \leq 6$ and $m \geq 23$
2. $7 \leq k \leq 27$ and $m \geq 4k - 1$
3. $7 \leq k \leq 27$ and $27 \leq m \leq 4k - 2$
4. $k \geq 28$ and $m \geq 19$
5. $7 \leq m \leq 18$ and $26 \leq k \leq 4m - 2$
6. $2 \leq m \leq 18$ and $k \geq \max\{4m - 1, 28\}$

In Sections 6.4 and 6.5 we consider consider Region four. In Section 6.6 we consider Regions one, two, and six. Then in Section 6.7 we consider Regions three and five. Finally in Section 6.8 we prove Theorems 6.1.1 and 6.1.2.

The majority of proofs in this chapter have the following form. Let G and M be as in Theorem 6.1.1. For $x \in G \backslash M$ we construct $y = c_1 \dots c_t \in M$ such that the following hold.

(i) If $G = \mathrm{S}_n$ then y has odd parity, and if $G = \mathrm{A}_n$ then y has even parity.

(ii) $H := \langle x, y \rangle$ is transitive.

(iii) There exists $1 \leq i \leq t$ such that $l(c_i^{\mathcal{H}})$ has relatively few prime divisors (often a product of two primes).

(iv) There exists $r \in \mathbb{N}$ such that y^r is a Jordan element.

We assume that H is imprimitive with non-trivial block system $\mathcal{H}$. We then show that for each divisor d of $l(c_i^{\mathcal{H}})$, setting $l(c_i^{\mathcal{H}}) = d$ yields a contradiction. Hence by Lemma 4.2.10 it follows that H is primitive. Since H contains a Jordan element by Part (iv), it follows that $\mathrm{A}_n \leq H$, and so $H = G$ by Part (i).

6.2 General notation and preliminaries

We begin by defining the notation for the remainder of this chapter.

Notation 6.2.1. Let $m, k \geq 2$ and $n = mk \geq 12$, let $G = \mathrm{S}_n$ or A_n act on $\Omega = \{1, 2, \ldots, n\}$. For $1 \leq i \leq m$ let

$$\Omega_i = \{(i-1)k + 1, \ldots, ik\},$$

let $\mathcal{M} = \{\Omega_1, \ldots, \Omega_m\}$, and let $M = \mathrm{Stab}_G(\mathcal{M}) \cong (\mathrm{S}_k \,\mathrm{wr}\, \mathrm{S}_m) \cap G$. Then $\mathcal{M}$ is unique non-trivial block system for M. Let $x \in G \backslash M$.

Let $\mathcal{J}_t, \mathcal{J}_c, \mathcal{J}_s$ and $\mathcal{J}_w$ be as in Definition 4.3.3, and let $\mathcal{J} \subseteq \mathrm{S}_n$ be as in Theorem 4.3.4.

For $m, k \geq 7$, let p_m and p_k as in Theorem 4.4.1. Hence p_m and p_k are primes satisfying $\frac{m}{2} < p_m < m - 1$ and $\frac{k}{2} < p_k < k - 1$.

We use the following group to help divide the possibilities for $x \in G \backslash M$ into cases.

Definition 6.2.2. Let

$$\hat{M} = \Big(\mathrm{Sym}(\Omega_1 \cup \Omega_2) \times \mathrm{Sym}(\Omega_3) \times \cdots \times \mathrm{Sym}(\Omega_m)\Big) \cap G.$$

We now prove a useful property of elements in $\hat{M} \backslash M$.

Lemma 6.2.3. *Let $x \in \hat{M} \backslash M$. Then for $1 \leq i \leq m$ there exist (not necessarily distinct) $\lambda_i, \lambda_i^x \in \Omega_i$.*

Proof. Since $x \in \hat{M}$ it follows that $(\Omega_1 \cup \Omega_2)^x = \Omega_1 \cup \Omega_2$ and $\Omega_i^x = \Omega_i$ for $3 \leq i \leq m$. If $\Omega_1^x = \Omega_2$ then $\Omega_2^x = \Omega_1$ and so $x \in M$, a contradiction. Hence $\Omega_1^x \cap \Omega_1 \neq \emptyset$ and so $\Omega_2^x \cap \Omega_2 \neq \emptyset$. Thus there exists $\lambda_1, \lambda_1^x \in \Omega_1$ and $\lambda_2, \lambda_2^x \in \Omega_2$. Since $x \in \hat{M}$ every $\lambda_i \in \Omega_i$ satisfies $\lambda_i^x \in \Omega_i$ for $3 \leq i \leq m$. □

Recall that M is a maximal coclique in $\Gamma(G)$ exactly when for all $x \in G\backslash M$ there exists $y \in M$ such that $\langle x, y\rangle = G$. We now prove results which enable us to consider fewer possibilities for $x \in G\backslash M$.

In the remaining results of this section we use the following notation.

Notation 6.2.4. For $z \in G\backslash M$, let $S(z) = \mathrm{Supp}(z)$, let $S_i(z) = \Omega_i \cap S(z)$ for $1 \leq i \leq m$ and let $\mathcal{S}(z) = \{1 \leq i \leq m \mid \Omega_i^z \neq \Omega_i\}$.

Proposition 6.2.5. *Let G, M and $\mathcal{M}$ be as in Notation 6.2.1, let $x \in G\backslash M$, and let X_1 and X_2 be as defined below. Then either x or x^{-1} is M-conjugate to an element of X_1 and to an element of X_2.*

(i) *X_1 is the set of elements $z \in G\backslash M$ such that $1^z = k+1$, $\Omega_1^z \notin \mathcal{M}$ and $|S_1(z)| \geq |S_2(z)|$.*

(ii) *X_2 is the set of elements $z \in G\backslash M$ such that $1^z = k+1$ and if $i \in \mathcal{S}(z)$ then $|S_1(z)| \geq |S_i(z)|$.*

Proof. (i) Since $x \notin M$ there exist distinct i and j such that $\Omega_i^x \cap \Omega_j \neq \emptyset$ and $\Omega_i^x \neq \Omega_j$. Hence there exists $\alpha \in \Omega_i$ such that $\alpha^x \in \Omega_j$. Equivalently $\Omega_j^{x^{-1}} \cap \Omega_i \neq \emptyset$, $\Omega_j^{x^{-1}} \neq \Omega_i$, $\alpha^x \in \Omega_j$ and $(\alpha^x)^{x^{-1}} \in \Omega_i$. Hence, by interchanging x, α, Ω_i with $x^{-1}, \alpha^{-1}, \Omega_j$ if necessary, we can assume that $|S_i(x)| \geq |S_j(x)|$.

By Lemma 4.1.8 there exists $g \in M$ such that $\alpha^g = 1$ and $(\alpha^x)^g = k+1$. Hence $\Omega_i^g = \Omega_1$ and $\Omega_j^g = \Omega_2$, and so $x^g \in X_1$.

(ii) Since $x \notin M$ it follows that $\mathcal{S}(x) \neq \emptyset$. Let $i \in \mathcal{S}(x)$ be such that $|S_i(x)| \geq |S_l(x)|$ for all $l \in \mathcal{S}(x)$. Since $\Omega_i^x \neq \Omega_i$ there exists $j \neq i$ and $\alpha \in \Omega_i$ such that $\alpha^x \in \Omega_j$. By Lemma 4.1.8 there exists $g \in M$ such that $\alpha^g = 1$ and $(\alpha^x)^g = k+1$. Hence $\Omega_i^g = \Omega_1$ and $\Omega_j^g = \Omega_2$, and so $x^g \in X_2$. □

Proposition 6.2.6. *Let G, M and $\mathcal{M}$ be as in Notation 6.2.1, let $\hat{M}$ be as in Definition 6.2.2, let X_1 and X_2 be as in Proposition 6.2.5, and let Z_i and Z_i' for $1 \leq i \leq 5$ be as defined below. If $x \in Z_i$ then x is M-conjugate to an element of Z_i'.*

(i) *If $m \geq 3$, then $Z_1 = X_1\backslash\hat{M}$ and $Z_1' = \{z \in X_1 \mid 3 \in \mathcal{S}(z)\}$.*

(ii) *If $m \geq 4$ then*
$Z_2 = \{z \in X_1 \mid S(z) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for some $3 \leq i, j \leq m\}$ and
$Z_2' = \{z \in X_1 \mid S(z) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$ and $|S_3(z)| \geq |S_4(z)|\}$.

(iii) *If $m \geq 5$ then $Z_3 = X_1\backslash Z_2$ and Z_3' is the set of elements $z \in X_1$ for which there* *exists $s \geq 5$ such that*

$$0 < |S_i(z)| \leq |S_{i+1}(z)| \text{ for } 3 \leq i \leq s-1, \quad \text{and } |S_i(z)| = 0 \text{ for } i > s.$$

(iv) *If $m \geq 5$ then $Z_4 = \{z \in X_1 \mid z \notin \hat{M}$ and $|S_1(z)| = 1\}$ and Z_4' is the set of elements $z \in X_1$ such that there exists $\alpha \in \Omega_3$ such that $\alpha^z \in \Omega_1 \cup \Omega_4$,*

$$|S_i(z)| \geq |S_{i+1}(z)| \quad \text{for } 5 \leq i \leq m-1,$$

and if $m \geq 7$ and $|S_7(z)| \geq 1$ then there exists $\beta \in S_5(z)$ and $\gamma \in S_6(z)$ such that $\beta^z \neq \gamma$.

(v) *If $m \geq 3$ then $Z_5 = X_2 \backslash \hat{M}$ and $Z_5' = \{z \in X_2 \mid 3 \in \mathcal{S}(z)\}$.*

Proof. Observe that if $g \in M$ fixes Ω_1 and Ω_2 pointwise then $X_1^g = X_1$ and $X_2^g = X_2$.

(i)&(v) Let $l = 1$ or 5 and let $x \in Z_l$. If $(\Omega_1 \cup \Omega_2)^x = \Omega_1 \cup \Omega_2$, then $x \notin \hat{M}$ implies that there exists $3 \leq i \leq m$ such that $i \in \mathcal{S}(x)$. If $(\Omega_1 \cup \Omega_2)^x \neq \Omega_1 \cup \Omega_2$ then there exists $3 \leq i \leq m$ such that $(\Omega_1 \cup \Omega_2)^x \cap \Omega_i \neq \emptyset$, and so $i \in \mathcal{S}(x)$. By Lemma 4.1.8 there exists $g \in M$ which fixes Ω_1 and Ω_2 pointwise and sends Ω_i to Ω_3. Hence $x^g \in Z_l'$.

(ii) Let $x \in Z_2$. Then there exist $3 \leq i, j \leq m$ such that $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$. By Lemma 4.1.8 there exist $g, h \in M$ which fix Ω_1 and Ω_2 pointwise and satisfy $\Omega_i^g = \Omega_3 = \Omega_j^h$ and $\Omega_j^g = \Omega_4 = \Omega_i^h$. Hence either x^g or x^h is in Z_2'.

(iii) Let $x \in Z_3$ and let $I = (i_1, \ldots, i_a, i_{a+1}, \ldots, i_{m-2})$ be an ordering of $\{3, \ldots, m\}$ such that

$$0 < |S_{i_j}(x)| \leq |S_{i_{j+1}}(x)| \text{ for } 1 \leq j \leq a-1, \quad \text{and } |S_{i_j}(x)| = 0 \text{ for } j > a.$$

Since $x \in Z_3$ it follows that $a \geq 3$. By Lemma 4.1.8 there exists $g \in M$ fixing Ω_1 and Ω_2 pointwise and mapping Ω_{i_j} to Ω_{j+2} for $1 \leq j \leq a$, and so $x^g \in Z_3$.

(iv) Let $x \in Z_4$. Then by the definition of X_1, $|S_2(x)| = 1$. Since $x \notin \hat{M}$, the argument in (i) proves that there exists an $3 \leq i \leq m$ such that $i \in \mathcal{S}(x)$. Thus there exists $j \neq i$ and $\alpha \in \Omega_i$ such that $\alpha^x \in \Omega_j$. Since $\alpha \in \Omega_i \neq \Omega_1$ it follows that $\alpha \neq 1$, and so $\alpha^x \neq k+1$. Therefore from $|S_2(x)| = 1$, we deduce that $\alpha^x \notin \Omega_2$, and so $j \neq 2, i$.

Let $T = \{1, \ldots, m\} \backslash \{1, 2, i, j\}$ and let $t = |T|$. Let $(l_1, \ldots, l_t)$ be an ordering of the points in T such that

$$|S_{l_s}(x)| \geq |S_{l_{s+1}}(x)| \text{ for } 1 \leq s \leq t-1. \tag{6.1}$$

Now suppose that $|S_{l_2}(x)|, |S_{l_3}(x)| \geq 1$. If $|S_{l_1}(x)| \geq 2$ then let $\gamma \in S_{l_2}(x)$ and let $\beta \in S_{l_1}(x)\backslash\{\gamma^{x^{-1}}\}$. If $|S_{l_1}(x)| = 1$ then $|S_{l_2}(x)| = |S_{l_3}(x)| = 1$ by (6.1). Let $\beta \in S_{l_1}(x)$. Then either $\beta^x \notin \Omega_{l_2}$ or $\beta^x \notin \Omega_{l_3}$. Hence, by exchanging l_2 and l_3 if necessary, (6.1) is still satisfied, $\beta^x \notin \Omega_{l_2}$ and there exists $\gamma \in S_{l_2}(x)$.

If $j = 1$ then $\{1, 2, i, j\} = \{1, 2, j\}$, and so $t = m - 3$. By Lemma 4.1.8 there exists $g \in M$ such that g fixes Ω_1 and Ω_2 pointwise, $\Omega_i^g = \Omega_3$, $\Omega_{l_s}^g = \Omega_{4+s}$ for $1 \leq s \leq t-1$ and $\Omega_{l_t}^g = \Omega_4$. Otherwise $1, 2, i$ and j are distinct and so $t = m - 4$. By Lemma 4.1.8 there exists $g \in M$ such that g fixes Ω_1 and Ω_2 pointwise, $\Omega_i^g = \Omega_3$, $\Omega_j^g = \Omega_4$ and $\Omega_{l_s}^g = \Omega_{4+s}$ for $1 \leq s \leq t$. In either case, relabel α^g, β^g and γ^g as α, β and γ. Hence $x^g \in Z_4$. □

We now define two distinct hypothesis which between them cover all possibilities.

Hypothesis 6.2.7. *Let* $n \geq 12$

(A) *Let* $G = \mathrm{A}_n$ *if* n *is odd and* $G = \mathrm{S}_n$ *if* n *is even.*

(B) *Let* $G = \mathrm{A}_n$ *if* n *is even and* $G = \mathrm{S}_n$ *if* n *is odd.*

In both cases, let M *be as in Notation 6.2.1.*

Proposition 6.2.8. *Let* G, M, k, m *and* $\mathcal{J}$ *be as in Notation 6.2.1, let* X_1 *and* X_2 *be as in Proposition 6.2.5, let* $Z_1, \ldots, Z_5$ *be as in Proposition 6.2.6, let* $\mathcal{Z} = \cup_{i=1}^5 Z_i$ *and let* $\mathcal{Z}' = \cup_{i=1}^5 Z_i'$.

(i) *If* k *and* m *are as in Regions three or five of Figure 6.1 then let*

$$X = \{x \in X_2 \mid x \in \mathcal{Z}' \text{ or } x \notin \mathcal{Z}\},$$

(ii) *if* $2 \leq k \leq 7$, $m \geq 13$ *and* $x \in \mathcal{J}$ *then*

$$X = \{x \in X_1 \mid x \in \mathcal{Z}' \text{ or } x \notin \mathcal{Z}\},$$

(iii) *otherwise let*

$$X = \{x \in (X_2 \cap \mathcal{J}) \cup (X_1 \backslash \mathcal{J}) \mid x \in \mathcal{Z}' \text{ or } x \notin \mathcal{Z}\}.$$

Then M *is a maximal coclique in* $\Gamma(G)$ *if and only if for all* $x \in X$ *there exists* $y \in M$ *such that* $\langle x, y\rangle = G$.

Proof. Recall that M is a maximal coclique in $\Gamma(G)$ if and only if for all $x \in G\backslash M$ there exists $y \in M$ such that $\langle x, y\rangle = G$.

In each case $X \subseteq G\backslash M$, and so the forward direction is clear. So assume that M is not a maximal coclique in $\Gamma(G)$. Therefore there exists $x \in G\backslash M$ such that $\langle x, y\rangle \neq G$ for all $y \in M$. Hence $\langle x^g, y^g \rangle \neq G^g = G$ for all $g \in G$. Therefore if there exists $g \in M$ such that $x^g \in X$ then the result follows.

Since $x \in \mathcal{J}$ if and only if the cycle type or size of support of x satisfy certain properties, it follows that $x \in \mathcal{J}$ if and only if $x^g \in \mathcal{J}$ for all $g \in M$. Consider Case (iii), the other two cases are almost identical. First consider $x \in \mathcal{J}$. By Proposition 6.2.5 there exists $g \in M$ such that $x^g \in X_2$. If $x^g \notin \mathcal{Z}$ then $x^g \in X$, and if $x^g \in \mathcal{Z}$ then by Proposition 6.2.6 there exists $h \in M$ such that $x^{gh} \in \mathcal{Z}'$, and so $x^{gh} \in X$. Now consider $x \notin \mathcal{J}$. Then by Proposition 6.2.5 there exists $g \in M$ such that $x^g \in X_1$. If $x^g \notin \mathcal{Z}$ then $x^g \in X$, if $x^g \in \mathcal{Z}$ then by Proposition 6.2.6 there exists $h \in M$ such that $x^{gh} \in \mathcal{Z}'$ and so $x^{gh} \in X$. □

6.3 $x \in \mathcal{J}$

In this section, we prove the following theorem.

Theorem 6.3.1. *Let n, G and M be as in Hypothesis 6.2.7. If either $k \geq 8$ or $m \geq 13$, and if $x \in (G \cap \mathcal{J})\backslash M$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

We first prove that Theorem 6.3.1 holds under Hypothesis 6.2.7(A).

6.3.1 Hypothesis 6.2.7(A)

Recall that X_2 is the set of elements $x \in G\backslash M$ such that $1^x = k+1$, and for $1 \leq i \leq m$ if $\Omega_i^x \neq \Omega_i$, then $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_i \cap \mathrm{Supp}(x)|$.

First assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$.

Lemma 6.3.2. *Let n, G and M be as in Hypothesis 6.2.7(A). If $x \in X_2 \cap \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Since $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$ there exists $\alpha \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{1\}$. By Lemma 4.2.1, an element of S_n composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. Hence we may let $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{1 \cdot (k-1)}_{\Theta_1 \cup \Theta_2 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_3^{\mathcal{M}}) = m-1}$$

and $\{\alpha\} = \Theta_1$. Let $H = \langle x, y \rangle$ and let $Y = \langle y \rangle$. Then $\alpha \in \Theta_1$, $1 \in \Theta_2$, $k+1 \in \Theta_3$ and $\alpha^x \in \Theta_2 \cup \Theta_3$, and so H is transitive. Assume for a contradiction that Δ is a non-trivial block for H and $\alpha \in \Delta$.

Since Δ is non-trivial, there exists $\beta \in \Delta\backslash\{\alpha\}$. From $\alpha^y = \alpha$, it follows that $\Delta^y = \Delta$, and so $\beta^Y \subseteq \Delta$. If $\beta \in \Theta_3$, then $\Theta_3 \subseteq \Delta$ and so $|\Delta| \geq (m-1)k + 1 > \frac{n}{2}$, a contradiction. Hence assume that $\Delta \cap \Theta_3 = \emptyset$, and so $\beta \in \Theta_2$ and $\Delta = \Theta_1 \cup \Theta_2 = \Omega_1$. We reach a contradiction by Lemma 4.2.14(iv) since $\Theta_3 = \Omega_2 \cup \cdots \cup \Omega_m$ and $\mathcal{M} \backslash \{\Omega_2, \ldots, \Omega_m\} = \{\Omega_1\} \subseteq \mathcal{H}$.

Thus H is a primitive group containing $x \in \mathcal{J}$, and so $\mathrm{A}_n \leq H$ by Theorem 4.3.4. By the parity of y it follows that $H = G$. □

The next lemma shows the existence of an element of S_n satisfying certain properties, we then give an example of such an element. Recall that for $\alpha \in \Omega$, we write $\Omega(\alpha)$ to denote the block in $\mathcal{M}$ which contains α.

Lemma 6.3.3. *Let n, G and M be as in Hypothesis 6.2.7(A), let $x \in X_2$ such that $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, and let $A := \{\alpha \in \Omega \mid \alpha^x \notin \Omega(\alpha)\}$. Then there exists and n-cycle $y \in M$ satisfying all of the following.*

(i) *$\langle x, y\rangle$ is transitive.*

(ii) *$l(y^{\mathcal{M}}) = m$.*

(iii) *$A = \{1^{y^i} \mid 0 \leq i \leq |A| - 1\}$.*

(iv) *For $\alpha \in A$, either $\alpha^{xy^{-1}} = \alpha$ or $\alpha^{x^{-1}y} = \alpha$.*

(v) *If $\beta \in \mathrm{Supp}(x)$ and $\beta^x \in \Omega(\beta)$, then either $\beta^{xy^{-m}} = \beta$ or $\beta^{x^{-1}y^m} = \beta$.*

Proof. Let $S = \big\{i \in \{1, 2, \ldots, m\} \bigm| \Omega_i^x \neq \Omega_i\big\}$ and let $T = \{1, \ldots, m\} \backslash S$. Since $1^x = k + 1$, it follows that $1, 2 \in S$. If $i \in S$, then from $x \in X_2$ it follows that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_i \cap \mathrm{Supp}(x)|$, and so $|\Omega_i \cap \mathrm{Supp}(x)| = 1$. If $i \in T$ then $\Omega_i^x = \Omega_i$. Hence we may define

$$c := x|_{\bigcup_{i \in S} \Omega_i} \quad \text{and} \quad d_i := x|_{\Omega_i} \ \text{ for } \ i \in T.$$

Therefore $\mathrm{Supp}(c) = A$ and $x = c \cdot \prod_{i \in T} d_i$.

Let $\mathcal{Y} \subseteq G$ be the set of n-cycles of M. Then Conditions (i) and (ii) hold for all $y \in \mathcal{Y}$. Let $c = c_1 c_2 \cdots c_t$ be the decomposition of c into disjoint non-trivial cycles, and let l_j denote the length of c_j. Then $l_1 + \cdots + l_t = |A|$. Let $c_j = (\alpha_{j,1}, \alpha_{j,2}, \ldots, \alpha_{j,l_j})$ for $1 \leq j \leq t$, and if necessary relabel $c_1, \ldots, c_t$ such that $\alpha_{1,1} = 1$. Since $y^{\mathcal{M}}$ is an m-cycle, it follows that $\{1^{y^i} \mid 0 \leq i \leq m - 1\}$ contains exactly one point of each M-block. Hence we may let $\emptyset \neq \mathcal{Y}_1 \subseteq \mathcal{Y}$ be such that $y \in \mathcal{Y}_1$ if and only if

$$\alpha_{j,u}^y = \begin{cases} \alpha_{j,u+1} & \text{if } 1 \leq j \leq t \text{ and } 1 \leq u \leq l_j - 1, \\ \alpha_{j+1,1} & \text{if } 1 \leq j < t \text{ and } u = l_j. \end{cases}$$

Hence if $y \in \mathcal{Y}_1$ then y satisfies Condition (iii). In addition, $\alpha_{j,u}^{xy^{-1}} = \alpha_{j,u}$ for $1 \leq u \leq l_j - 1$ and $\alpha_{j,l_j}^{x^{-1}y} = \alpha_{j,l_j}$, and so $y \in \mathcal{Y}_1$ satisfies Condition (iv).

For $i \in T$ let $d_i = e_{i,1}e_{i,2}\cdots e_{i,r_i}$, be the decomposition of d_i into disjoint non-trivial cycles, and label the lengths $w_{i,1},\ldots,w_{i,r_i}$ respectively. Then $w_{i,1}+\cdots+w_{i,r_i} = |\mathrm{Supp}(d_i)|$. Let $e_{i,j} = (\beta_{i,j,1},\beta_{i,j,2},\ldots,\beta_{i,j,w_{i,j}})$. By Condition (ii) it follows that $\mathrm{Supp}(d_i) \subseteq \Omega(\beta_{i,1,1}) = \beta_{i,1,1}^{\langle y^m\rangle}$ for all $y \in \mathcal{Y}_1$. Hence we may let $\mathcal{Y}_2 \subseteq \mathcal{Y}_1$ such that $y \in \mathcal{Y}_2$ if and only if for all $i \in T$

$$\beta_{i,j,u}^{y^m} = \begin{cases} \beta_{i,j,u+1} & \text{if } 1 \le j \le r_i, \text{ and } 1 \le u \le w_{i,j}-1, \\ \beta_{i,j+1,1} & \text{if } 1 \le j < r_i, \text{ and } u = w_{i,j}. \end{cases}$$

Let $y \in \mathcal{Y}_2$ and let $\beta_{i,j,u} \in \mathrm{Supp}(d_i)$. If $1 \le u \le w_{ij}-1$, then $\beta_{i,j,u}^{xy^{-m}} = \beta_{i,j,u}$; and if $2 \le u \le w_{ij}$, then $\beta_{i,j,u}^{x^{-1}y^m} = \beta_{i,j,u}$. Thus y satisfies Condition (v) and so satisfies the lemma. □

Example 6.3.4. Let $m = 7$ and $k = 3$ so that $\Omega_1 = \{1,2,3\}$, $\Omega_2 = \{4,5,6\},\ldots,$ and $\Omega_7 = \{19,20,21\}$. If $x = (1,5,7)(10,14)(16,17)$, then $S = \{1,2,3,4,5\}$, $T = \{6,7\}$ and

$$x = c\cdot d_6 \cdot d_7 = (1,5,7)(10,14)\cdot(16,17)\cdot \mathrm{id}.$$

One possible y would be

$$y = (1,5,7,10,14,16,19,2,4,8,11,13,17,20,3,6,9,12,15,18,21).$$

Then $y^{\mathcal{M}} = (\Omega_1,\Omega_2,\Omega_3,\Omega_4,\Omega_5,\Omega_6,\Omega_7)$. We see that

$$A = \{1,5,7,10,14\} = \{1^i \mid 1 \le i \le 5\}$$

and $\alpha^{xy^{-1}} = \alpha$ for $\alpha \in \{1,5,10\}$, and $\alpha^{x^{-1}y} = \alpha$ for $\alpha \in \{7,14\}$. In addition, $\mathrm{Supp}(d_6) = \{16,17\}$ and $16^{xy^{-7}} = 16$ and $17^{x^{-1}y^7} = 17$. △

Proposition 6.3.5. *Let n, G and M be as in Hypothesis 6.2.7*(A)*. If $x \in X_2 \cap \mathcal{J}$, then there exists $y \in M$ such that $\langle x,y\rangle = G$.*

Proof. If $|\Omega_1 \cap \mathrm{Supp}(x)| \ge 2$, then the result holds by Lemma 6.3.2. Hence we may assume that $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ and let A be as in Lemma 6.3.3.

Let $y \in M$ be as in Lemma 6.3.3 and let $H = \langle x,y\rangle$. Hence H is transitive by Lemma 6.3.3(i). For a contradiction, let Δ be a non-trivial block for H with $1 \in \Delta$.

If $\Delta \cap \mathrm{Fix}(x) \neq \emptyset$, then $\Delta^x = \Delta$ and so $1^x, 1^{x^{-1}} \in \Delta$. By Lemma 6.3.3(iv) either $1^{xy^{-1}} = 1$ or $1^{x^{-1}y} = 1$, and so it follows that $\Delta^y = \Delta$. Thus $\Delta^H = \Delta$, and so $\Delta = \Omega$, a contradiction.

Suppose that Δ contains $\beta \in \mathrm{Supp}(x)\backslash A$. Then $\beta^x \in \Omega(\beta)$. Let $\Sigma := \Delta^{y^m}$, and $\Gamma := \Delta^{y^{-m}}$ so that $1^{y^m}, \beta^{y^m} \in \Sigma$ and $1^{y^{-m}}, \beta^{y^{-m}} \in \Gamma$. By Lemma 6.3.3(ii) $l(y^{\mathcal{M}}) = m$, and so $1^{y^m}, 1^{y^{-m}} \in \Omega_1\backslash\{1\}$, and by assumption $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$. Hence $\Sigma^x = \Sigma$ and $\Gamma^x = \Gamma$. Therefore $\beta^{y^m x^{-1}} \in \Sigma$ and $\beta^{y^{-m}x} \in \Gamma$. By Lemma 6.3.3(v), either $\beta^{xy^{-m}} = \beta$ or $\beta^{x^{-1}y^m} = \beta$, and so either $\beta = \beta^{y^m x^{-1}} \in \Sigma\cap\Delta$ or $\beta = \beta^{y^{-m}x} \in \Gamma\cap\Delta$. Hence either $\Delta = \Sigma$ or $\Delta = \Gamma$. A contradiction since $\Delta \subseteq \mathrm{Supp}(x)$, $1^{y^m} \in \Sigma \cap \mathrm{Fix}(x)$ and $1^{y^{-m}} \in \Gamma \cap \mathrm{Fix}(x)$. Hence $\Delta \subseteq A$.

Assume instead that $\alpha \in (\Delta \cap A)\backslash\{1\}$. Then by Lemma 6.3.3(iii) $\alpha = 1^{y^l}$ for some $1 \leq l < |A| \leq m$. Therefore $\Delta^{y^l} = \Delta$ and so $1^{y^{-l}} \in \Delta$. A contradiction since $1^{y^{-l}} \notin A$.

Hence H is primitive. Since $x \in \mathcal{J}$ it follows that $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

6.3.2 Hypothesis 6.2.7(B)

Here we show that Theorem 6.3.1 holds under Hypothesis 6.2.7(B). This parity causes more difficulty, and so we divide into more cases. Even so the proofs are fairly technical and dense, but matters will improve somewhat in Section 6.4. We split into the following three regions which we depicted below. Hence we consider a larger range of m and k than described in Theorem 6.3.1.

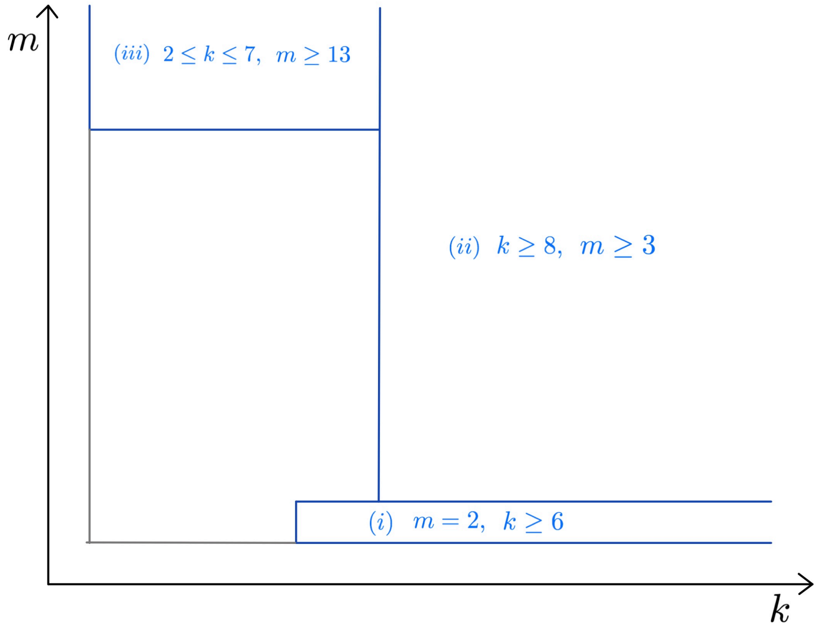

m
(iii) $2 \leq k \leq 7$, $m \geq 13$
(ii) $k \geq 8$, $m \geq 3$
(i) $m = 2$, $k \geq 6$
k

Figure 6.2: Patchwork Proof - Division of m and k into regions.

Region (i) - $m = 2$ and $k \geq 6$

Observe that since $m = 2$, it follows by Hypothesis 6.2.7(B) that $G = \mathrm{A}_n$. We begin with a preliminary lemma.

Lemma 6.3.6. *Let $m = 2$, let $k \geq 6$, and let G and M be as in Hypothesis 6.2.7*(B)*. If*

$x \in X_2 \cap \mathcal{J}$, then either there exist $\alpha, \alpha^x \in \Omega_1 \cap \mathrm{Supp}(x)$; or there exists $\beta \in \Omega_1 \cap \mathrm{Fix}(x)$ and $\gamma \in \Omega_1$ such that $\gamma^x \in \Omega_2 \backslash \{k+1\}$.

Proof. Since $\Omega_1^x \neq \Omega_1$ and $m = 2$, it follows that $\Omega_2^x \neq \Omega_2$. Hence $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$ by the definition of X_2. From $G = \mathrm{A}_n$ we deduce that $|\mathrm{Supp}(x)| \geq 3$, and so there exists $\gamma \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$.

Since $x \notin M$ it follows that $\Omega_1^x \neq \Omega_2$ and so $\Phi := \Omega_1^x \cap \Omega_1 \neq \emptyset$. If $\Phi \cap \mathrm{Supp}(x) \neq \emptyset$ then there exists $\alpha, \alpha^x \in \Omega_1 \cap \mathrm{Supp}(x)$, and the result holds. Hence assume that $\Phi \subseteq \mathrm{Fix}(x)$ and let $\beta \in \Phi$. It follows that $\gamma^x \in \Omega_2$, and since $\gamma \neq 1$ we deduce that $\gamma \neq k+1$. □

Lemma 6.3.7. *Let $m = 2$, let $k \geq 6$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_2 \cap \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Let α, β and γ be as in Lemma 6.3.6. By Lemma 4.2.1, a product of two cycles is in $G = \mathrm{A}_n$. Based on α, β and γ we split into three cases, although all will follow a similar structure. We begin with a general argument.

Let $y = c_1c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{2 \cdot 2(k-1)}_{l(y^{\mathcal{M}})=2},$$

such that $H = \langle x, y \rangle$ is transitive. Let $\epsilon := \Theta_1 \cap \Omega_1$ and $\zeta := \Theta_1 \cap \Omega_2$. Assume by way of a contradiction that H is imprimitive and let Δ be a non-trivial block for H containing ϵ.

If $\zeta \in \Delta$, then $\Delta^y = \Delta$. Hence if $\Delta \cap \Theta_2 \neq \emptyset$, then $\Delta = \Omega$, a contradiction. If $\zeta \notin \Delta$ then there exists $\eta \in \Delta \cap \Theta_2$. Hence $\Delta = \{\epsilon\} \cup \eta^{\langle y^2 \rangle}$. If $\eta \in \Omega_1$, then $\Delta = \Omega_1$ and so $\mathcal{H} = \mathcal{M}$, a contradiction since $x \notin M$. Hence either $\Delta = \{\epsilon, \zeta\}$ or $\Delta = \{\epsilon\} \cup \Omega_2 \backslash \{\zeta\}$.

In all cases we show that both possibilities for Δ lead to a contradiction. Hence it will follow that H is primitive, and since $x \in \mathcal{J}$ the result will follow by Theorem 4.3.4.

First assume that there exist β, γ as in Lemma 6.3.6. Let $y = c_1c_2 \in M$, with $\mathcal{C}(y) = 2 \cdot 2(k-1)$ and $\Theta_1 = \{\beta, k+1\}$. Let $H = \langle x, y \rangle$. Then $k+1 \in \Theta_1$ and $1 \in \Theta_2$, and so H is transitive. Let Δ be a non-trivial block for H containing β. Since $\beta \in \mathrm{Fix}(x)$ and $k+1 \in \mathrm{Supp}(x)$ it follows that $\Delta \neq \{\beta, k+1\}$. If $\Delta = \{\beta\} \cup \Omega_2 \backslash \{k+1\}$, then $\Delta^y = \{k+1\} \cup \Omega_1 \backslash \{\beta\}$. Since $\beta \in \mathrm{Fix}(x)$ we deduce that that Δ, and so Δ^y also, is fixed by x. This gives a contradiction since $\gamma \in \Omega_1 \backslash \{1\} \subseteq \Delta^y$ and $\gamma^x \in \Omega_2 \backslash \{k+1\} \subseteq \Delta$. Hence the result follows by the above.

Now suppose that there exists $\alpha, \alpha^x \in \Omega_1 \cap \mathrm{Supp}(x)$ and let $\epsilon := (k+1)^x$. We split into two cases, first assume that $\alpha^x = 1$ and $\epsilon \in \Omega_2$. Let $y = c_1c_2 \in M$ with $\mathcal{C}(y) = 2 \cdot 2(k-1)$

and $\Theta_1 = \{\alpha, k+1\}$ and $1^y = \epsilon$. Since $k+1 \in \Theta_1$ and $1 \in \Theta_2$, it follows that $H = \langle x, y\rangle$ is transitive. Let Δ be a non-trivial block for H with $\alpha \in \Delta$. If $\Delta = \{k+1, \alpha\}$, then $\Delta^x = \{\alpha^x, (k+1)^x\} = \{1, \epsilon\}$. From $1^y = \epsilon$ we deduce that $(\Delta^x)^y = \Delta^x$, and so $|\Delta^x| \geq n-2 > 2$, a contradiction. If $\Delta = \{\alpha\} \cup \Omega_2 \backslash \{k+1\}$, then $\Delta^y = \{k+1\} \cup \Omega_1 \backslash \{\alpha\}$. Hence $1, k+1 \in \Delta^y$ and so $(\Delta^y)^x = \Delta^y$. Thus $1^{x^{-1}} = \alpha \in \Delta \cap \Delta^y$, a contradiction. Hence the result follows by the above.

Finally assume that there exists $\alpha, \alpha^x \in \Omega_1 \cap \mathrm{Supp}(x)$, and either $\alpha^x \neq 1$ or $(k+1)^x \in \Omega_1$. Let $y = c_1c_2 \in M$ with $\mathcal{C}(y) = 2 \cdot 2(k-1)$ such that $\Theta_1 = \{\alpha^x, k+1\}$, in addition if $\alpha^x \neq 1$ then $\alpha^{y^2} = 1$. Hence $\alpha^x \in \Theta_1$ and $\alpha \in \Theta_2$, and so $H = \langle x, y\rangle$ is transitive. Let Δ be a non-trivial block for H containing α^x.

First assume that $\alpha^x = 1$, and so $(k+1)^x \in \Omega_1$ and $1^x = k+1 = 1^y$. If $\Delta = \{1, k+1\}$, then $\Delta = \Delta^H = \Omega$, a contradiction. If $\Delta = \{1\} \cup \Omega_2 \backslash \{k+1\}$, then $\Delta^y = \{k+1\} \cup \Omega_1 \backslash \{1\}$. Since $\alpha \in \Omega_1$ it is immediate that $\alpha \neq k+1$ and so $\alpha^x \neq (k+1)^x$. Thus from $\alpha^x = 1$ and $(k+1)^x \in \Omega_1$ we deduce that $(k+1)^x \in \Omega_1 \backslash \{1\}$. Hence $k+1, (k+1)^x \in \Delta^y$ and so $(\Delta^y)^x = \Delta^y$. Therefore $1 = (k+1)^{x^{-1}} \in \Delta \cap \Delta^y$, a contradiction.

Now assume that $\alpha^x \neq 1$ and so $\alpha^{y^2} = 1$. If $\Delta = \{\alpha^x, k+1\}$ then $\Delta^{x^{-1}} = \{\alpha, 1\}$. Hence $1^{\langle y^2 \rangle} \subseteq \Delta^{x^{-1}}$ and so $|\Delta^{x^{-1}}| \geq k-2 > 2$, a contradiction. If $\Delta = \{\alpha^x\} \cup \Omega_2 \backslash \{k+1\}$, then $\Delta^y = \{k+1\} \cup \Omega_1 \backslash \{\alpha^x\}$. Then $1, k+1 \in \Delta^y$ and it follows that $(\Delta^y)^x = \Delta^y$, a contradiction since $\alpha \in \Delta^y$ and $\alpha^x \in \Delta$. Thus the result follows by the above. Hence the lemma holds in all cases. □

Region (ii) - $k \geq 8$ and $m \geq 3$

We split into four cases: first that $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 4$; then into two cases when $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$; and then finally the general case of this subsection.

Lemma 6.3.8. *Let $m \geq 3$, let $k \geq 5$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_2 \cap \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 4$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. Since $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 4$, there exists $\alpha \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$ and $\beta \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1, \alpha, \alpha^x\}$. By Lemma 4.2.1 an element composed of four cycles lies in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4$ of M such that

$$\mathcal{C}(y) = \underbrace{1 \cdot 1 \cdot (k-2)}_{\Theta_1 \cup \Theta_2 \cup \Theta_3 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_4^M) = m-1}$$

with $\{\alpha\} = \Theta_1$ and $\{\beta\} = \Theta_2$. For each $y \in \mathcal{Y}$, let $H = H(y) = \langle x, y\rangle$ and let $Y = \langle y\rangle$. Then $1 \in \Theta_3$, $k+1 \in \Theta_4$, $\alpha^x \in \Theta_3 \cup \Theta_4$ and $\beta^x \in \Theta_1 \cup \Theta_3 \cup \Theta_4$, hence H is transitive. Assume, by way of a contradiction, that H is an imprimitive group with non-trivial block system $\mathcal{H}$.

Let $\Delta \in \mathcal{H}$ with $\alpha \in \Delta$. Since $|\Delta| > 1$ there exists $\gamma \in \Delta \backslash \{\alpha\}$. From $\alpha^y = \alpha$ we deduce that $\Delta^y = \Delta$, and so $\gamma^Y \subseteq \Delta$. If $\gamma \in \Theta_4$, then $\Theta_4 \subseteq \Delta$, and so $|\Delta| > \frac{n}{2}$, a contradiction. Hence we may assume that $\Delta \cap \Theta_4 = \emptyset$ and so $\Delta \subseteq \Omega_1$.

Since $\Theta_4 = \Omega_2 \cup \cdots \cup \Omega_m$, Lemma 4.2.14(iv) implies that $\mathcal{M}\backslash\{\Omega_2, \ldots, \Omega_m\} = \{\Omega_1\} \nsubseteq \mathcal{H}$, and so in particular $\Delta \neq \Omega_1$. Thus either $\Delta = \Omega_1 \backslash \{\beta\}$ or $\Delta = \{\alpha, \beta\}$. If $\Delta = \Omega_1 \backslash \{\beta\}$, then there exists $\Gamma \in \mathcal{H} \backslash \{\Delta\}$ with $\beta \in \Gamma$ and $\Gamma \cap \Theta_4 \neq \emptyset$. Since $\beta^y = \beta$ it follows as for Δ that $|\Gamma| > \frac{n}{2}$, a contradiction. Therefore $\Delta = \{\alpha, \beta\}$ and $\Delta^x = \{\alpha^x, \beta^x\}$. If $\beta^x = \alpha$ then $\Delta = \Delta^x$ and so $\Delta = \Delta^H = \Omega$, a contradiction. Hence $\beta^x \neq \alpha$ and so $\Delta^x \subseteq \Theta_3 \cup \Theta_4$. Let $z_1 := y^{\frac{|\Theta_3|}{2}}$ and $z_2 := y^{\frac{|\Theta_4|}{2}}$. Since $|\Theta_4| > |\Theta_3|$ and $\Delta^x \subseteq \Theta_3 \cup \Theta_4$, Lemma 4.2.14(v) implies that either $\Delta^x \subseteq \Theta_3$ or $\Delta^x \subseteq \Theta_4$. From $|\Delta^x| = 2$ it follows that if $\Delta^x \subseteq \Theta_3$ then $\Delta^{xz_1} = \Delta^x$, and if $\Delta^x \subseteq \Theta_4$ then $\Delta^{xz_2} = \Delta^x$. If $\alpha^x, \beta^x \in \Theta_3$, then since $k \geq 3$ there exists $y \in \mathcal{Y}$ such that $\alpha^{xz_1} \neq \beta^x$. If $\alpha^x, \beta^x \in \Theta_4$, then since $k \geq 3$ there exists $y \in \mathcal{Y}$ such that $\alpha^{xz_2} \neq \beta^x$. In either case we reach a contradiction.

Therefore H is primitive and contains $x \in \mathcal{J}$. Hence $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and by the parity of y it follows that $H = G$. □

Hence for the remainder of this subsection, we may assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$. We first prove two slightly more general lemmas which we also use in Section 6.7.

Recall that p_k is a prime with $\frac{k}{2} < p_k < k-1$, and by Lemma 4.4.13 for $k \geq 8$ there exists $p_k \leq k-2$. In addition, if $\alpha \in \Omega$ then $\Omega(\alpha)$ is the M-block which contains α.

Lemma 6.3.9. *Let $k \geq 8$, let $m \geq 3$, and let G and M be as in Hypothesis 6.2.7*(B). *Assume that $x \in X_2$, $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \nsubseteq \Omega_1 \cup \Omega_2$. Then for all $p_k < k-2$, there exists $y \in M$ with cycle type $mp_k \cdot m(k-p_k)$ such that $\langle x, y\rangle$ is primitive.*

Proof. Since $\mathrm{Supp}(x) \nsubseteq \Omega_1 \cup \Omega_2$ there exist $\alpha, \alpha^x \in \mathrm{Supp}(x)$ such that $\alpha^x \notin \Omega_1 \cup \Omega_2$. Hence in particular $\alpha^x \neq k+1$, and so $\alpha \neq 1$. By Lemma 4.2.1, elements composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ such that $y^{\mathcal{M}}$ is an m-cycle with

$$\mathcal{C}(y) = \underbrace{mp_k \cdot m(k-p_k)}_{l(y^{\mathcal{M}})=m},$$

satisfying all of the following.

(i) $\alpha, 1, 1^y = k+1 \in \Theta_1$ and $\alpha^x \in \Theta_2$.

(ii) If $\alpha \notin \Omega_1 \cup \Omega_2$, then $1 = \alpha^y$; if $\alpha \in \Omega_1$, then $1 = \alpha^{y^m}$; and if $\alpha \in \Omega_2 \backslash \{k+1\}$, then $1 = \alpha^{y^{m-1}}$.

(iii) $\Omega_1 \cap \Theta_1 \subseteq \{1, \alpha\} \cup \mathrm{Fix}(x)$.

(iv) Let $B_1 := (\Omega_1 \cap \mathrm{Supp}(x))\backslash\{1,\alpha\}$ and $B_i := \{\beta \in \Omega_i\backslash\{1,k+1,\alpha\} \mid \beta^x \notin \Omega_i\}$ for $2 \leq i \leq m$. Require that $B_1, B_2, \ldots, B_m \subseteq \Theta_2$.

(v) For $2 \leq i \leq \frac{mp_k}{2}$ let $\gamma_i := 1^{y^i}$, and require that $\gamma_i^x \in \Theta_1 \cap \Omega(\gamma_i)$.

We first justify why $\mathcal{Y} \neq \emptyset$. Condition (i) can easily been seen to hold, and Condition (ii) also since $y^{\mathcal{M}}$ is an m-cycle and $\Omega_1^{y^{\mathcal{M}}} = \Omega_2$. Since $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $x \in X_2$, it follows that if $\Omega_i^x \neq \Omega_i$ then $|\Omega_i \cap \mathrm{Supp}(x)| \leq 3$. Therefore the sets B_1 and B_i for $2 \leq i \leq m$ all have size at most $3 \leq k - p_k$. Hence we can insist that $B_1, B_2, \ldots, B_m \subseteq \Theta_2$. Therefore Conditions (iii) and (iv) can be satisfied. Now consider Condition (v). By Condition (iv) it follows that $\gamma_i^x \in \Omega(\gamma_i)$ automatically, and so we can let $\gamma_i^x \in \Theta_1 \cap \Omega(\gamma_i)$.

Since $\alpha \in \Theta_1$ and $\alpha^x \in \Theta_2$ it follows that for each $y \in \mathcal{Y}$ the group $H = H(y) = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H is an imprimitive group with non-trivial block system $\mathcal{H} = \mathcal{H}\langle x, y\rangle$.

Since $p_k \nmid (k - p_k)$ it follows that $l(c_1^{\mathcal{H}}) \neq p_k m$ by Lemma 4.2.14(ii). Since $|\Theta_1| > \frac{n}{2}$ it follows that $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). Hence we may let Δ and Γ be distinct blocks of $\mathcal{H}$ with $1 \in \Delta$ and $k+1 \in \Gamma$.

Let d be a divisor of m. If $l(c_1^{\mathcal{H}}) = d$, then $\Omega_1 \cap \Theta_1 \subseteq \Delta$ by Lemma 4.2.13(ii). Therefore by Condition (iii), Δ contains a point of $\Omega_1 \cap \mathrm{Fix}(x)$, and so $\Delta^x = \Delta$. Hence $k+1 \in \Delta$, a contradiction since $k+1 \in \Gamma$. Therefore, for the remainder of the proof we may assume that the length of $c_1^{\mathcal{H}}$ does not divide m.

Assume that $l(c_1^{\mathcal{H}}) = p_k$. By the above we may assume that $p_k \nmid m$ and so $\gcd(p_k, m) = 1$. We first show that if $\alpha \in \Gamma$ then we reach a contradiction. If $\alpha \notin \Omega_1 \cup \Omega_2$, then let $j := 2$; if $\alpha \in \Omega_1$, then let $j := m+1$; and if $\alpha \in \Omega_2$, then let $j := m$. Hence by Conditions (i) and (ii) it follows that $\alpha^{y^j} = k+1$ and so $\Gamma^{y^j} = \Gamma$ and $\delta := 1^{y^{j+1}} = (k+1)^{y^j} \in \Gamma$. Since $3 \leq j+1 \leq m+2 < \frac{mp_k}{2}$, Condition (v) implies that $\delta^x \in \Theta_1$, and so $\Gamma^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$. Since $\alpha^x \in \Theta_2$ and $p_k \nmid |\Theta_2|$, we reach a contradiction by Lemma 4.2.14(iii). Hence $\alpha \notin \Gamma$. Since $\gcd(p_k, m) = 1$, Lemma 4.2.13(iv) implies that $|\Gamma \cap \Omega_i \cap \Theta_1| = 1$ for $1 \leq i \leq m$. In particular, Γ contains a point of $\Omega_1 \cap \Theta_1\backslash\{1, \alpha\} \subseteq \mathrm{Fix}(x)$, and so $\Gamma^x = \Gamma$. Hence $1 = (k+1)^{x^{-1}} \in \Gamma$, a contradiction since $1 \in \Delta \neq \Gamma$.

Now let $1 < e < m$ be a divisor of m, and assume that $l(c_1^{\mathcal{H}}) = ep_k$. Then $\epsilon := 1^{y^{ep_k}} \in \Delta$. Since $1 \in \Delta$ and $k+1 \in \Gamma$ it follows that $\Delta^x = \Gamma$, and so $\epsilon^x \in \Gamma$. Since $ep_k \leq \frac{mp_k}{2}$, Condition (v) implies that $\epsilon^x \in \Theta_1 \cap \Omega(\epsilon)$. Hence $\epsilon^x = \epsilon^{y^{cm}}$ for some $c \in \mathbb{N}$, and so

$$(k+1)^{y^{ep_k+cm-1}} = 1^{y^{ep_k+cm}} = \epsilon^{y^{cm}} = \epsilon^x. \tag{6.2}$$

Since $k+1, \epsilon^x \in \Gamma$, Equation (6.2) implies that $\Gamma^{y^{ep_k+cm-1}} = \Gamma$. From $l(c_1^{\mathcal{H}}) = ep_k$ we deduce that $\Gamma^{y^{ep_k}} = \Gamma$. Hence

$$\Gamma^{y^{ep_k+cm-1}} = \Gamma = \Gamma^{y^{ep_k}}.$$

Therefore ep_k divides $cm-1$, a contradiction since $e \mid m$ and $e > 1$.

Therefore H is primitive. □

Lemma 6.3.10. *Let $k \geq 8$, let $m \geq 3$, and let G and M be as in Hypothesis 6.2.7*(B)*. Assume that $x \in X_2$, $|\mathrm{Supp}(x)| \geq 4$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$. Then for each prime $p_k < k-2$, there exists $y \in M$ with cycle type $mp_k \cdot m(k-p_k)$ such that $\langle x, y\rangle$ is primitive.*

Proof. If $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2$ then the result holds by Lemma 6.3.9. Hence we may assume that $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$. Since $x \in X_2$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$. Since $|\mathrm{Supp}(x)| \geq 4$ there exists $\alpha \in \mathrm{Supp}(x)\backslash\{1, k+1, 1^{x^{-1}}\}$, and so in particular $\alpha^x \neq 1, k+1$. By Lemma 4.2.1, elements composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{mp_k \cdot m(k-p_k)}_{l(y^{\mathcal{M}})=m}$$

such that $1, 1^y = k+1, \alpha \in \Theta_1$, $\alpha^y \in \mathrm{Fix}(x)$ and $\mathrm{Supp}(x)\backslash\{1, k+1, \alpha\} \subseteq \Theta_2$. We briefly justify why $\mathcal{Y} \neq \emptyset$. From $1^y = k+1$ it follows that $\Omega_1^y = \Omega_2$. If $\alpha \in \Omega_2$ then since $m \geq 3$ it follows that $\alpha^y \notin \Omega_1 \cup \Omega_2$, and so $\alpha^y \in \mathrm{Fix}(x)$ automatically. If $\alpha \in \Omega_1$, then $\alpha^y \in \Omega_2$. Since $k \geq 7$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$, it is possible to ensure that $\alpha^y \in \Omega_2 \cap \mathrm{Fix}(x)$. The last condition is possible since $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$, $|\Omega_i\backslash\{1, k+1, \alpha\} \cap \mathrm{Supp}(x)| \leq 2$ for $i = 1, 2$ and $k - p_k \geq 2$. This condition implies that $\alpha^x \in \Theta_2$, hence $H = \langle x, y\rangle$ is a transitive group. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$.

Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$. Since $mp_k > m(k-p_k)$ it follows by Lemma 4.2.14(v) that Δ contains $\beta \in \Theta_1\backslash\{1\}$. Since $1^y = k+1 = 1^x$ it follows that $\Delta^{xy^{-1}} = \Delta$. Hence if $\beta \in \mathrm{Fix}(x) \cup \{k+1\}$, then $\Delta = \Omega$ a contradiction. Therefore we may assume that $\beta \in \mathrm{Supp}(x)\backslash\{1, k+1\}$, and so $\beta = \alpha$. Hence $1^y, \alpha^y \in \Delta^y$. Since $\alpha^y \in \mathrm{Fix}(x)$ it follows that $(\Delta^y)^x = \Delta^y$. Therefore $1^{yx^{-1}} = 1 \in \Delta^y$, and so $(\Delta^y)^y = \Delta^y$. Hence $\Delta^y = (\Delta^y)^H = \Omega$, a contradiction. Therefore H is primitive. □

Using the three previous lemmas we can now complete the proof of Theorem 6.3.1 in the case of Hypothesis 6.2.7(B) and Region (ii)

Lemma 6.3.11. *Let $k \geq 8$, let $m \geq 3$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_2 \cap \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. First assume that $|\mathrm{Supp}(x)| \geq 4$. If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 4$, then the result holds by Lemma 6.3.8. If $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$, then by Lemma 6.3.10 there exists a product of two cycles $y \in M$ such that $\langle x, y \rangle$ is primitive. Hence by Theorem 4.3.4 and the parity of y, it follows that $\langle x, y \rangle = G$.

If $|\mathrm{Supp}(x)| = 2$, then $x = (1, k+1)$ and $G = \mathrm{S}_n$. Let $y \in M$ is an n-cycle with $1^x = k+1$. Then $\langle x, y \rangle = G$.

Hence we may assume that $|\mathrm{Supp}(x)| = 3$. Thus there exists $\alpha \in \mathrm{Supp}(x)$ such that $x = (1, k+1, \alpha)$. Let $y = c_1 c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{m \cdot m(k-1)}_{l(y^{\mathcal{M}})=m}$$

such that $1, 1^y = k+1 \in \Theta_1$ and $\alpha \in \Theta_2$. Let $H = \langle x, y \rangle$. Then it is clear that H is transitive. Assume for a contradiction that Δ is a non-trivial block for H and $1 \in \Delta$. By Lemma 4.2.14(v) it follows that $\Delta \neq \{1, \alpha\}$. Hence Δ contains a point of $\Omega \backslash \{1, \alpha\} = \{k+1\} \cup \mathrm{Fix}(x)$. Since $1 \in \Delta$ and $1^x = k+1 = 1^y$, it follows that $\Delta = \Delta^H = \Omega$, a contradiction.

Therefore H is primitive. Since $x \in \mathcal{J}$ it follows that $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

Region (iii) - $2 \leq k \leq 7$ and $m \geq 13$

In this subsection we let $x \in X_1$. Hence $1^x = k+1$, $\Omega_1^x \notin \mathcal{M}$, and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$.

We divide into three cases: first $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$; second $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$; and then the general case. Finally we prove Theorem 6.3.1.

We begin with two preliminary lemmas.

Lemma 6.3.12. *Let $k \leq 7$, let $m \geq 13$, and let $x \in X_1$. If*

$$\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\},$$

then there exist distinct points α, β satisfying the following:

(i) *$\Omega(\alpha) \neq \Omega(\beta)$;*

(ii) *$\beta \in \mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\})$; and*

(iii) *if* $\alpha \in \mathrm{Supp}(x)$, *then* $\alpha^x, \beta^x \notin \Omega_1 \cup \Omega_2$.

Proof. First suppose that $\mathrm{Fix}(x) \subseteq \Omega_1 \cup \Omega_2$. Since $m \geq 13$ there exists $\alpha \in \Omega\backslash(\Omega_1 \cup \Omega_2 \cup \Omega_1^{x^{-1}} \cup \Omega_2^{x^{-1}})$ and $\beta \in \Omega\backslash(\Omega_1 \cup \Omega_2 \cup \Omega_1^{x^{-1}} \cup \Omega_2^{x^{-1}} \cup \Omega(\alpha))$. Hence $\alpha \in \mathrm{Supp}(x)$, $\Omega(\alpha) \neq \Omega(\beta)$, $\beta \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\})$ and $\alpha^x, \beta^x \notin \Omega_1 \cup \Omega_2$.

Now suppose that $\mathrm{Fix}(x) \nsubseteq \Omega_1 \cup \Omega_2$. Let $i \in \{3, \ldots, m\}$ such that $|\Omega_i \cap \mathrm{Fix}(x)| \geq |\Omega_l \cap \mathrm{Fix}(x)|$ for $3 \leq l \leq m$. Let $\alpha \in \Omega_i \cap \mathrm{Fix}(x)$. By the maximality of $|\Omega_i \cap \mathrm{Fix}(x)|$ and since $\mathrm{Supp}(x) \nsubseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$, there exist $j \neq 1, 2, i$ and $\beta \in (\Omega_j \cap \mathrm{Supp}(x))\backslash(\Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\})$. Hence $\Omega(\alpha) \neq \Omega(\beta)$ and $\beta \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\})$. □

Recall that p_m is a Bertrand prime with $\frac{m}{2} < p_m < m - 1$. The following lemma will be used to show that an element $y \in M$ is well defined.

Lemma 6.3.13. *Let* $m \geq 13$*, let* $k \leq 7$*, let* $p_m \geq 11$*, and let* $n = mk$*. Then the set of integers* S*, as defined below, are distinct modulo* n*. If* $k = 2$ *then let*

$$T \in \Big\{\{0, k, 2k, p_m, p_m + k, p_m + 2k\}, \{0, k, 2k, 2k + 1\}\Big\},$$

if $k \geq 3$ *then let*

$$T \in \Big\{\{0, k, 2k, k + p_m, 2k + p_m, 2k + 2p_m, (m + 1)k - p_m\}, \{0, k, 2k, k + 1, 2k + 1\}\Big\},$$

and let

$$S = \begin{cases} T \cup \{2p_m\} & \textit{if } k = 4, \\ T \cup \{2p_m, 3p_m\} & \textit{if } k = 6, \\ T & \textit{otherwise.} \end{cases}$$

Proof. Since $p_m \geq 11$ it follows that $p_m > k$. We begin by claiming that all elements of $T\backslash\{k - p_m\}$ are positive and less than $n = mk$. In all cases

$$T \subseteq \{0, k, k + 1, 2k, 2k + 1, p_m, p_m + k, p_m + 2k, 2p_m + 2k, (m + 1)k - p_m\}.$$

Since $p_m > k$ it follows that

$$0 < k < k + 1 < 2k < 2k + 1 \leq p_m + k < p_m + 2k < 2p_m + 2k \text{ and} \tag{6.3}$$

$$k < p_m < p_m + k.$$

For all k we have

$$p_m + 2k \leq m - 2 + 2(7) = m + 12 < 2m \leq n,$$

and if $k \geq 3$ then $3p_m < k(m-1)$ and so

$$2p_m + 2k < (m+1)k - p_m < mk.$$

The claim then follows since $2p_m + 2k, (m+1)k - p_m \in T$ only if $k > 3$.

Hence elements of T are congruent modulo n if and only if they're equal. Note that $2k+1$ and $p_m + k$ are never simultaneously in T, also p_m is never in the same set as $k+1$ or $2k+1$; and $p_m \neq 2k$ since p_m is odd. Hence in all cases all elements of T are distinct. Therefore if $k \neq 4, 6$ then the result follows.

Let $k = 4$ or 6. Now $p_m + k < 2p_m < 2p_m + 2k$, and $2p_m \neq p_m + 2k$ since one is even and one is odd. Hence by (6.3) it follows that $2p_m \notin T$, and so $T \cup \{2p_m\}$ contains no duplications. Hence the result holds for $k = 4$. Now let $k = 6$. Then

$$p_m + 2k < 3p_m \quad \text{and} \quad 3p_m < (m+1)6 - p_m = (m+1)k - p_m.$$

Since p_m is odd it follows that $3p_m \neq 2p_m + 2k$. Hence by (6.3) it follows that $3p_m \notin T \cup \{2p_m\}$, and so $T \cup \{2p_m, 3p_m\}$ contains no duplications. □

Lemma 6.3.14. *Let $m \geq 13$, let $k \leq 7$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_1 \cap \mathcal{J}$ and* $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$*, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Let α and β be as in Lemma 6.3.12. Since $m \geq 13$, it follows that there exists $p_m \geq 11$. Hence Lemma 6.3.13 holds, $p_m > k$ and $\gcd(p_m, k) = 1$.

By Lemma 4.2.1, elements composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1 c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_m k}_{\substack{l(c_1^{\mathcal{M}})=p_m \\ \Omega_1,\Omega(\alpha),\Omega(\beta),\Omega(\alpha^x),\Omega(\beta^x)\in\mathrm{Supp}(c_1^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_2^{\mathcal{M}})=m-p_m \\ \Omega_2\in\mathrm{Supp}(c_2^{\mathcal{M}})}}$$

satisfying the following.

(i) If 2 is a proper divisor of k, then let $\gamma := 1^{y^{2pm}}$ and require that $\gamma^x \in \Theta_1 \cup \{(k+1)^{y^{(m-pm)}}\}$. If 3 is a proper divisor of k, then let $\delta := 1^{y^{3pm}}$ and require that $\delta^x \in \Theta_1 \cup \{(k+1)^{y^{-(m-pm)}}\}$.

(ii) $1^{y^k} = \alpha$ and $1^{y^{2k}} = \beta$.

(a) If $\alpha^x = \alpha$, then we require the following to hold. If $\beta^x \in \Omega_1$, then $\beta^x = 1^{y^{pm}}$; if $\beta^x \in \Omega(\alpha)$, then $\beta^x = 1^{y^{pm+k}} = \alpha^{y^{pm}}$; if $\beta^x \in \Omega(\beta)$, then $\beta^x = 1^{y^{pm+2k}} = \beta^{y^{pm}}$; otherwise $\beta^x = 1^{y^{2k+1}} = \beta^y$.

(b) If $\alpha^x \neq \alpha$, then instead we require the following to hold.

(1) If $k = 2$ and $\Omega(\alpha), \Omega(\alpha^x), \Omega(\beta)$ and $\Omega(\beta^x)$ are distinct, then either $\alpha^{xy} = \beta^x$ or $\beta^{xy} = \alpha^x$.

(2) If $k > 2$, then the following hold.

- If $\Omega(\alpha^x) = \Omega(\beta^x)$, then $(\alpha^x)^{y^{p_m}} = \beta^x$.

- If $\{\Omega(\alpha^x), \Omega(\beta^x)\} = \{\Omega(\alpha), \Omega(\beta)\}$, then

$$\{\alpha^x, \beta^x\} = \{\alpha^{y^{p_m}}, \beta^{y^{2p_m}}\} = \{1^{y^{k+p_m}}, 1^{y^{2k+2p_m}}\}.$$

- Otherwise, either $\alpha^x = \beta^{xy}$ or $\beta^x = \alpha^{xy}$.

We justify why $\mathcal{Y}$ is non-empty. We first check that 1^{y^i} is not defined to be more than one point. Then we check that each point is placed in the correct M-block.

Let $R = \{i \mid 1^{y^i}$ is defined for $y \in \mathcal{Y}\}$. Then by Lemma 6.3.13 it follows that the elements of R are distinct modulo n.

If $\epsilon \in \Theta_1$ then $\Omega(\epsilon) = \epsilon^{\langle y^{p_m}\rangle}$. Hence α^x and β^x are placed in the correct M-blocks. If $\epsilon \in \Theta_2$ then $\Omega(\epsilon) = \epsilon^{\langle y^{(m-p_m)}\rangle}$. If $\gamma^x \notin \Omega_2$ then since $p_m \geq 11$ we can let $\Omega(\gamma^x) \in \mathrm{Supp}(c_1^{\mathcal{M}})$ and so $\gamma^x \in \Theta_1$. If $\gamma^x \in \Omega_2$ then we may let $\gamma^x = (k+1)^{y^{p_k(m-p_m)}} \in \Omega_2$. Similarly for δ.

Since $1 \in \Theta_1$ and $k+1 \in \Theta_2$ it follows that $H = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $Y = \langle y\rangle$ and let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $|\Theta_1| > \frac{n}{2}$ and $p_m k \nmid |\Theta_2|$, it follows that $l(c_1^{\mathcal{H}}) \neq 1$ and $l(c_1^{\mathcal{H}}) \neq p_m k$ by Lemma 4.2.14(i) and (ii) respectively.

Suppose that $l(c_1^{\mathcal{H}}) = p_m$. From $p_m \nmid |\Theta_2|$, Lemma 4.2.11(iv) implies that $\Delta \cap \Theta_2 = \emptyset$. Hence block size is k and so $l(c_2^{\mathcal{H}}) = m - p_m$. Therefore $\mathcal{H}$ is the set of translates under y of $1^{\langle y^{p_m}\rangle}$ and $(k+1)^{\langle y^{(m-p_m)}\rangle}$. Since $\Omega_1 = 1^{\langle y^{p_m}\rangle}$ and $\Omega_2 = (k+1)^{\langle y^{(m-p_m)}\rangle}$, it follows that $\mathcal{H} = \mathcal{M}$, a contradiction since $x \notin M$.

Let $1 < d < k$ be a divisor of k. Then $d = 2$ or 3. Assume that $l(c_1^{\mathcal{H}}) = dp_m$. Since $p_m \nmid |\Theta_2|$ it follows that $\Delta \subseteq \Theta_1$ and so $|\Delta| = \frac{k}{d}$. By Condition (i), Δ contains either γ or δ. Suppose that $\gamma \in \Delta$, the argument for δ is very similar. Let $\Gamma := \Delta^x$, so that $k+1, \gamma^x \in \Gamma$. If $\gamma^x \in \Theta_1$, then $c_1^{\mathcal{H}} = c_2^{\mathcal{H}}$ by Lemma 4.2.11(i), a contradiction since $\Delta \subseteq \Theta_1$. If $\gamma^x = (k+1)^{y^{(m-p_m)}}$, then $\Gamma^{y^{(m-p_m)}} = \Gamma$, and so $(k+1)^{\langle y^{p_k(m-p_m)}\rangle} = (k+1)^{\langle y^{(m-p_m)}\rangle} = \Omega_2 \subseteq \Gamma$. Thus $|\Gamma| \geq k > \frac{k}{d}$, a contradiction.

Finally assume that $l(c_1^{\mathcal{H}}) = e$ for $e > 1$ a divisor of k. Then $1, \alpha, \beta \in \Delta$ and $k + 1, \alpha^x, \beta^x \in \Delta^x$. We begin by assuming that Δ^x is fixed by either y, y^{p_m} or y^{k+p_k}, and derive a contradiction. Since $\gcd(p_m, (m-p_m)k) = 1$, it follows that $(k+1)^{\langle y^{p_m} \rangle} = (k+1)^Y$, and since $\gcd(k + p_m, p_m k) = 1$ it follows that $\alpha^{\langle y^{k+p_k} \rangle} = \alpha^Y$. Therefore if y^{p_m} or y^{k+p_m} fix Δ^x then it follows that y fixes Δ^x. Thus $\Omega = \Theta_1 \cup \Theta_2 = \alpha^Y \cup (k + 1)^Y \subseteq \Delta^x$, a contradiction.

If $\alpha^x = \alpha$, then $\Delta = \Delta^x$ and so $1, \alpha, \beta, k + 1, \alpha^x, \beta^x \in \Delta$. Hence by Condition (ii)(a), either $(\Delta^x)^{y^{p_m}} = \Delta^x$ or $(\Delta^x)^y = \Delta^x$, and so we reach a contradiction. Now assume that $\alpha^x \neq \alpha$. If $k > 2$ then by Condition (ii)(b)(2) there exists $i \in \{1, p_m, k + p_m\}$ such that $\{\alpha^x, \beta^x\}^{y^i} \cap \{\alpha^x, \beta^x\} \neq \emptyset$. Hence Δ^x is fixed by y, y^{p_m} or y^{k+p_m}, and so we reach a contradiction by the above.

Hence we may now assume that $k = 2$. Therefore $e = 2$, and $c_1^{\mathcal{H}} = (\Delta, \Sigma)$ for some $\Sigma \in \mathcal{H}$. Thus $|\Delta \cap \Theta_1| = p_m$, and since $p_m \nmid n$ it follows that $y^{\mathcal{H}} = (\Delta, \Sigma)$. Then $\Delta^x = \Delta$ and $\Sigma^x = \Sigma$, since $\mathrm{Fix}(x) \neq \emptyset$ by Lemma 4.3.5. Hence $\alpha^x, \beta^x \in \Delta$. We now show that there exists and odd integer t such that either $\alpha^x = \alpha^{y^t}$ or $\beta^x = \beta^{y^t}$ or $\alpha^{xy^t} = \beta^x$. Hence it will follows that Γ contains either α^x or β^x, a contradiction.

Since $k = 2$, if $\epsilon \in \Theta_1$ then $\Omega(\epsilon) = \{\epsilon, \epsilon^{y^{p_m}}\}$. If $\alpha^x \in \Omega(\alpha) \cup \Omega(\beta)$ then automatically, either $\alpha^x = \alpha^{y^{p_m}}$ or $\alpha^x = \beta^{y^{p_m}} = \alpha^{y^{2+p_m}}$. If $\beta^x \in \Omega(\alpha) \cup \Omega(\beta)$ then again automatically, $\beta^x = \beta^{y^{p_m}}$ or $\beta^x = \alpha^{y^{p_m}} = \beta^{y^{-2+p_m}}$. If $\Omega(\alpha^x) = \Omega(\beta^x)$, then $\alpha^{xy^{p_m}} = \beta^x$. Otherwise, it follows by Condition (ii)(b)(1) that either $\alpha^{xy} = \beta^x$ or $\beta^{xy} = \alpha^x$. Hence the claim holds and we reach a contradiction.

Therefore H is a primitive group containing $x \in \mathcal{J}$, and so $H = G$ by Theorem 4.3.4. □

Lemma 6.3.15. *Let $m \geq 13$, let $k \leq 7$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_1 \cap \mathcal{J}$ and* $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$*, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $x = (1, k + 1)$, then $G = \mathrm{S}_n$. Let y be an n-cycle with $1^x = k + 1$, so that $\langle x, y \rangle = G$.

Hence we may assume that $|\mathrm{Supp}(x)| \geq 3$. If $k > 2$ then let $\alpha \in \mathrm{Supp}(x) \backslash \{1, k + 1\}$. If $k = 2$, then $\Omega_1 = \{1, 2\}$ and $\Omega_2 = \{3, 4\}$. From $1^x = 3$, $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$ and $|\mathrm{Supp}(x)| \geq 3$ it follows that $x \in \big\{(1, 3, 2), (1, 3, 4), (1, 3, 4, 2)\big\}$. Let $\alpha^x = 1$ so that $\alpha \neq 1, k + 1$. By Lemma 4.2.1, an element of S_n composed of two cycles lies in A_n if and only if $G = \mathrm{A}_n$. Hence we may let $\mathcal{Y}$ be the set of elements $y = c_1 c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{m \cdot m(k-1)}_{l(y^{\mathcal{M}})=m},$$

such that $\alpha \in \Theta_1$ and $1, 1^y = k+1, \alpha^x \in \Theta_2$. Hence $H = H(y) = \langle x, y\rangle$ is transitive. Assume by way of a contradiction that H is imprimitive with non-trivial block system $\mathcal{H}$.

Let Δ be the block of $\mathcal{H}$ containing 1 and let $\beta \in \Delta\backslash\{1\}$. Since $1^x = k+1 = 1^y$, it follows that $\Delta^y = \Delta^x$. If $\beta \in \Omega\backslash(\Omega_1 \cup \Omega_2)$ then $\beta \in \mathrm{Fix}(x)$, and so $\Delta^x = \Delta$. Hence $\Delta = \Delta^H = \Omega$, a contradiction. If $\beta \in \Omega_2$ then $\beta^y \in \Omega_2^y \subseteq \mathrm{Fix}(x)$, and so $(\Delta^y)^x = \Delta^y$. Thus $\Delta^y = (\Delta^y)^{x^{-1}} = \Delta^{xx^{-1}} = \Delta$, and so $\Delta = \Delta^H = \Delta$, a contradiction. Hence we may assume that $\beta \in \Omega_1$ and $\Delta \subseteq \Omega_1$.

If $\beta \in \Omega_1 \cap \Theta_1$, then $\beta^{y^m} = \beta$. Hence $\Delta^{y^m} = \Delta$ and $\{\beta\} \cup 1^{\langle y^m\rangle} \subseteq \Delta$. By the cycle type of y, it follows that $\Omega_1 = \{\beta\} \cup 1^{\langle y^m\rangle}$. Hence $\Delta = \Omega_1$, and by taking translates of Δ under y it follows that $\mathcal{H} = \mathcal{M}$, a contradiction.

Thus we may assume that $\beta \in \Omega_1 \cap \Theta_2$ and $\Delta \subseteq \Omega_1 \cap \Theta_2$. Hence by Lemma 4.2.11(i) no H-block contains points of both Θ_1 and Θ_2. Let $\Gamma \in \mathcal{H}$ with $\alpha \in \Gamma$. Then $\Gamma \subseteq \Theta_1$ and there exists $\gamma \in \Gamma\backslash\{\alpha\}$. If $\gamma \in \Omega\backslash(\Omega_1 \cup \Omega_2) \subseteq \mathrm{Fix}(x)$ then $\Gamma^x = \Gamma$, a contradiction since $\Gamma \subseteq \Theta_1$ and $\alpha^x \in \Theta_2$. Hence we may assume that $\Gamma \subseteq \Theta_1 \cap (\Omega_1 \cup \Omega_2)$. By the cycle type of y it follows that $|\Omega_i \cap \Theta_1| = 1$ for $i = 1, 2$, and since $1^y = k+1$ it follows that $\Omega_1^y = \Omega_2$. Hence $\Gamma^y = \Gamma$ and so $\Theta_1 \subseteq \Gamma$, a contradiction.

Therefore H is a primitive group containing $x \in \mathcal{J}$ and so $H = G$ by Theorem 4.3.4. □

Lemma 6.3.16. *Let $m \geq 13$, let $k \leq 7$, and let G and M be as in Hypothesis 6.2.7*(B)*. If $x \in X_1 \cap \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. If $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$, then the result holds by Lemma 6.3.14. If $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2$, then the result holds by Lemma 6.3.15. Hence we may assume that $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$ and there exists $\alpha \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \Omega_2)$.

By Lemma 4.2.1, an element of S_n composed of two cycles lies in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{m \cdot m(k-1)}_{l(y^{\mathcal{M}})=m}$$

satisfying the following.

(i) $1, 1^y = k+1 \in \Theta_1$.

(ii) Θ_1 contains exactly one of α, α^x.

(iii) $(\Omega_2\backslash\{k+1\})^y \cap \mathrm{Fix}(x) \neq \emptyset$.

(iv) There exists $\beta \in \Omega_2^{x^{-1}}\backslash\Omega_1$ such that β^y or $\beta^{y^{-1}} \in \Omega_1$.

We justify why $\mathcal{Y}$ is non-empty. If $\alpha^x \in \{1, k+1\}$, then let $\alpha \in \Theta_2$; and if $\alpha^x \notin \{1, k+1\}$, then let $\alpha \in \Theta_1$ and $\alpha^x \in \Theta_2$. Hence Condition (ii) can hold. Since $x \in X_1$, it follows that $\Omega_1^x \neq \Omega_2$ and so there exists $\beta \in \Omega_2^{x^{-1}}\backslash\Omega_1$. By Condition (i) $\Omega_1^y = \Omega_2$, and so if $\beta \in \Omega_2$, then $\beta^{y^{-1}} \in \Omega_1$. Otherwise let $\Omega(\beta)^y = \Omega_1$, then Condition (iv) holds. Since $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{1^{x^{-1}}\}$ and $m \geq 13$, there exists $\Omega_i \neq \Omega_1, \Omega_2, \Omega(\beta)$ and $\gamma \in \Omega_i \cap \mathrm{Fix}(x)$. Hence let $\gamma \in \Theta_2$ and $\Omega_2^y = \Omega_i$, so that Condition (iii) holds.

By Condition (ii), $H = H(y) = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$.

Let Δ be the block containing 1, and let $\delta \in \Delta\backslash\{1\}$. Then from $1^x = k+1 = 1^y$, it follows that $\Delta^y = \Delta^x$. Hence if $\delta \in \{k+1, 1^{x^{-1}}\} \cup \mathrm{Fix}(x)$ then $\Delta^x = \Delta$, and so $\Delta^H = \Delta$, a contradiction. Thus $\Delta \subseteq \mathrm{Supp}(x)\backslash\{1^{x^{-1}}, k+1\} \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}}\backslash\{k+1\}$. Since $1^{y^m} = 1$ it follows that $\delta^{\langle y^m\rangle} \subseteq \Delta$. Observe that if $\delta \in \Theta_2$, then by the cycle type of y it follows that $\delta^{y^{\langle m\rangle}} = \Omega(\delta) \cap \Theta_2$.

If $\delta \in \Omega_2\backslash\{k+1\}$, then $\delta \in \Theta_2$, and so $\delta^{\langle y^m\rangle} = \Omega_2 \cap \Theta_2 = \Omega_2\backslash\{k+1\}$. Hence $\Omega_2\backslash\{k+1\} \subseteq \Delta$ and so $\{k+1\} \cup (\Omega_2\backslash\{k+1\})^y \subseteq \Delta^y$. By Condition (iii) it follows that $\Delta^{yx} = \Delta^y$. Combining this with $\Delta^x = \Delta^y$ gives $\Delta^y = \Delta = \Delta^x$. Thus $\Delta = \Omega$, a contradiction.

Therefore we may assume that $\delta \in \Omega_1 \cup \Omega_2^{x^{-1}}$ and $\Delta \subseteq \Omega_1 \cup \Omega_2^{x^{-1}}$. If $\Delta \subseteq \Omega_1$, then $\delta \in \Omega_1\backslash\{1\} \subseteq \Theta_2$. Hence $\delta^{\langle y^m\rangle} = \Omega_1 \cap \Theta_2 = \Omega_1\backslash\{1\}$, and so $\Delta = \Omega_1$. By taking y translates of Δ we see that $\mathcal{H} = \mathcal{M}$, a contradiction. Hence there exists $\delta \in \Delta \cap (\Omega_2^{x^{-1}}\backslash\{1\})$, and so $\delta^x \in \Omega_2\backslash\{k+1\} \subseteq \Theta_2$ and $k+1, \delta^x \in \Delta^x \cap \Omega_2$. Now $(k+1)^{y^m} = k+1$ implies that $\{k+1\} \cup (\delta^x)^{\langle y^{pm}\rangle} = \Omega_2 \subseteq \Delta^x$. From $\Delta^x = \Delta^y$ we deduce that $\Omega_2^{y^{-1}} \cup \Omega_2^{x^{-1}} = \Omega_1 \cup \Omega_2^{x^{-1}} \subseteq \Delta$. Therefore $\Delta = \Omega_1 \cup \Omega_2^{x^{-1}}$ since $\Delta \subseteq \Omega_1 \cup \Omega_2^{x^{-1}}$. By Condition (iv) it follows that $\Delta^y = \Delta$, and so $\Delta = \Delta^y = \Delta^x$, a contradiction.

Therefore H is a primitive group containing $x \in \mathcal{J}$, and so $H = G$ by Theorem 4.3.4. □

Proof of Theorem 6.3.1.
By Proposition 6.2.8, we may assume that if Hypothesis 6.2.7(B) holds and n is as in Region (iii), then $x \in X_1$, and otherwise that $x \in X_2$.

If Hypothesis 6.2.7(A) holds, then the result follows from Proposition 6.3.5.

Suppose that Hypothesis 6.2.7(B) holds, and use the divisions of possibilities for m and k given in Figure 6.3.2. If n is in Region (i) then the result holds by Lemma 6.3.7. In Region (ii) the result follows from Lemma 6.3.11. In Region (iii) the result holds by Lemma 6.3.16. □

6.4 Hypothesis 6.2.7(A), Region four - $m \geq 19$, $k \geq 28$

In this section we prove the following proposition.

Proposition 6.4.1. *Let $m \geq 19$, let $k \geq 28$ and let G and M be as in Hypothesis 6.2.7*(A)*. Then for all $x \in X_1 \backslash \mathcal{J}$ there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Recall that X_1 is the set of elements $x \in G\backslash M$ such that $1^x = k+1$, $\Omega_1^x \notin \mathcal{M}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$. In addition we recall the definition

$$\hat{M} = \mathrm{Sym}(\Omega_1 \cup \Omega_2) \times \Omega_3 \times \cdots \times \Omega_m.$$

We first assume that the support of x is contained within few M-blocks. We then divide into two subsections - in the first we assume that $x \notin \hat{M}$, and in the second we assume that $x \in \hat{M}$.

Lemma 6.4.2. *Let $m \geq 19$, let $k \geq 28$ and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in X_1 \backslash \mathcal{J}$ and there exist $3 \leq i, j \leq m$ such that* $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$*, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Proposition 6.2.6(ii) we may assume that $\Omega_i = \Omega_3$ and $\Omega_j = \Omega_4$. By Lemma 4.2.1, an n-cycle is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of n-cycles $y \in M$ such that

$$\Omega_2^y = \Omega_1, \ \ \Omega_2^{y^2} = \Omega_3, \ \ \Omega_2^{y^3} = \Omega_5, \ \ \Omega_2^{y^4} = \Omega_4 \ \text{ and } \ \Omega_2^{y^5} = \Omega_6.$$

and $(k+1)^y = 1$. Since y is an n-cycle it is clear that $H = H(y) = \langle x, y\rangle$ is transitive. Let Δ be a non-singleton block for H containing $k+1$ and let $\alpha \in \Delta\backslash\{k+1\}$. Since $(k+1)^{yx} = 1^x = k+1$ it follows that $\Delta^{yx} = \Delta$. If $\alpha \in \mathrm{Supp}(x)\backslash\{1, k+1\} \subseteq \Omega_3 \cup \Omega_4$, then $\alpha^y \in \Omega_5 \cup \Omega_6 \subseteq \mathrm{Fix}(x)$, and so $\alpha^{yx} = \alpha^y \in \Delta \cap \mathrm{Fix}(x)$. Hence Δ contains a point of $\mathrm{Fix}(x)$ and $\{\alpha, \alpha^y\}$, and so $\Delta = \Delta^H = \Omega$.

Thus H is a primitive group containing an n-cycle and $|\mathrm{Supp}(x)| \leq 2 + 2k < \frac{19}{2}k < \frac{n}{2}$. Therefore by Theorem 4.3.7, it follows that $\mathrm{A}_n \leq H$, and so $H = G$ by the parity of y. □

6.4.1 $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$

Here we prove Proposition 6.4.1 under the assumption that $x \in X_1\backslash(\hat{M} \cup \mathcal{J})$. We first assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, and then prove the general case. We begin with two preliminary lemmas.

Lemma 6.4.3. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in X_1\backslash(\hat{M} \cup \mathcal{J})$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then one of the following holds.*

(i) *There exist $\alpha \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{1\}$ and distinct points $\beta, \gamma \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{\alpha\}$ such that $\Omega(\beta^x), \Omega(\gamma^x), \Omega_1$ are distinct.*

(ii) *There exists $\alpha \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{1\}$ and $\delta, \delta^x \in \Omega_1\backslash\{1, \alpha\}$ (with possibly $\delta = \delta^x$).*

Proof. First assume that $\Omega_1 \cap \Omega_1^x = \emptyset$, and so $\Omega_1 \subseteq \mathrm{Supp}(x)$. We show that (i) holds. Since $x \in X_1$ it follows that $\Omega_1^x \notin \mathcal{M}$, and so there exist $\beta, \gamma \in \Omega_1$ such that $\Omega(\beta^x) \neq \Omega(\gamma^x)$. From $\Omega_1^x \cap \Omega_1 = \emptyset$, it follows that none of $\Omega(\beta^x), \Omega(\gamma^x), \Omega_1$ are equal. Let $\alpha \in \Omega_1\backslash\{1, \beta, \gamma\}$, which exists because $k \geq 28$.

Now assume that $\Omega_1 \cap \Omega_1^x \neq \emptyset$. We show that (ii) holds. If $\Omega_1 \cap \mathrm{Fix}(x) \neq \emptyset$, then let $\delta = \delta^x \in \Omega_1 \cap \mathrm{Fix}(x)$ and let $\alpha \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{1\}$. Otherwise $\Omega_1 \subseteq \mathrm{Supp}(x)$ and so we let $\delta^x \in \Omega_1 \cap \Omega_1^x$ and $\alpha \in \Omega_1\backslash\{1, \delta, \delta^x\}$, again using $k \geq 28$. □

Lemma 6.4.4. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A). *If $x \in X_1\backslash(\mathcal{J} \cup \hat{M})$, then the following both hold.*

(i) *Either there exists $\alpha, \alpha^x \in \Omega_1$ or there exists $\beta \in \Omega_1\backslash\{1\}$ such that $\beta^x \notin \Omega_1 \cup \Omega_2$.*

(ii) *If there exist distinct Bertrand primes $p_k, p_k{}'$ and a Bertrand prime p_m such that $p_m \leq m-4$ and $p_k p_k{}' \mid (m-1)$, then there exist distinct points $\gamma, \gamma^x, \delta, \delta^x, \epsilon, \epsilon^x \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \Omega_2 \cup \Omega(\beta^x))$, and an element with cycle structure $1^{n-p_m k} \cdot p_m^k$ is in $\mathcal{J}_w$.*

Proof. Part (i) is immediate by the definition of X_1 since $\Omega_1^x \neq \Omega_2$.

We now prove Part (ii). We claim that $|\mathrm{Supp}(x)| \geq 6k+8$. Since $x \notin \mathcal{J}_s \subseteq \mathcal{J}$ and $p_k p_k{}' \mid (m-1)$ it follows that

$$\mathrm{Supp}(x) > 2(\sqrt{mk} - 1) > 2(\sqrt{p_k p_k{}' k} - 1).$$

We now show that $2(\sqrt{p_k p_k{}' k} - 1) \geq 6k + 8$, from which the claim will follow.

If $26 \leq k \leq 35$, then it can be verified using [33, Code 20] that $2(\sqrt{p_k p_k{}' k} - 1) \geq 6k+8$ for all distinct primes $p_k, p_k{}'$. Hence we may assume that $k \geq 36$. Let $y(k) = k^3 - 30k^2 - 115k - 100$. Then $y(k) > 0$ for $k \geq 36$. Therefore

$$k(k^2 + 6k + 5) = k^3 + 6k^2 + 5k > 36k^2 + 120k + 100 = (6k + 10)^2$$

and so

$$2\left(\sqrt{k \cdot \frac{k+1}{2} \cdot \frac{k+5}{2}} - 1\right) = \sqrt{k(k^2 + 6k + 5)} - 2 > 6k + 8.$$

Since p_k and $p_k{}'$ are distinct odd primes, it follows that $p_k \cdot p_k{}' \geq \frac{k+1}{2} \cdot \frac{k+5}{2}$, and so the claim follows.

Hence $|\mathrm{Supp}(x)| \geq 6k+8$. Let $T = (\Omega_1 \cup \Omega_1^{x^{-1}} \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \Omega(\beta^x) \cup \Omega(\beta^x)^{x^{-1}})$. Then $|\mathrm{Supp}(x)\backslash T| \geq 8$, and so there exist

$\gamma \in \mathrm{Supp}(x)\backslash T$, $\delta \in \mathrm{Supp}(x)\backslash(T \cup \{\gamma, \gamma^x, \gamma^{x^{-1}}\})$ and $\epsilon \in \mathrm{Supp}(x)\backslash(T \cup \{\gamma, \gamma^x, \gamma^{x^{-1}}, \delta, \delta^x, \delta^{x^{-1}}\})$.

Hence $\gamma, \gamma^x, \delta, \delta^x, \epsilon, \epsilon^x$ are as required.

We now verify that an element with cycle type $1^{n-p_m k} \cdot p_m^k$ is in $\mathcal{J}_w$ by Definition 4.3.2. Since $k \geq 8$, it suffices to show that $p_m > 2k-1$ and $n > (p_m+4)k-4$. Since $p_k p_k{}' \mid (m-1)$, it follows that $m > p_k p_k{}' > \frac{k}{2} \cdot \frac{k}{2} = \frac{k^2}{4}$. In addition $\frac{k^2}{8} \geq \frac{28k}{8} > 2k-1$, and so

$$p_m > \frac{m}{2} > \frac{k^2}{8} > 2k-1. \tag{6.4}$$

Finally, since $p_m \leq m-4$, it follows that

$$n = mk \geq (p_m+4)k > (p_m+4)k-4. \quad \square$$

Lemma 6.4.5. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A). *If $x \in X_1\backslash(\hat{M} \cup \mathcal{J})$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Lemma 4.4.15 there exist distinct primes p_k, $p_k{}'$ and p_m such that $p_m \leq m-4$.

First assume that $p_k p_k{}' \nmid (m-1)$ and, if necessary, relabel such that $p_k \nmid (m-1)$. Let α, β, γ or α, δ, δ^x be as in Lemma 6.4.3. By Lemma 4.2.1, an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(x) = \underbrace{p_k \cdot (k-p_k)}_{\Theta_1 \cup \Theta_2 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_3^{\mathcal{M}}) = m-1},$$

such that $1 \in \Theta_1$, $\alpha \in \Theta_2$, $\alpha^x \in \Theta_1 \cup \Theta_3$, and either $\delta, \delta^x \in \Theta_1$, or $\beta, \gamma \in \Theta_1$ and $\beta^{xy} = \gamma^x$. Hence $H = H(y) = \langle x, y\rangle$ is transitive. Assume, by way of contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$.

Since p_k divides neither $|\Theta_2|$ nor $|\Theta_3|$, it follows that $l(c_1^{\mathcal{H}}) \neq p_k$ by Lemma 4.2.14(ii). Hence $l(c_1^{\mathcal{H}}) = 1$ and so there exists $\Delta \in \mathcal{H}$ such that $\Theta_1 \subseteq \Delta$. Thus $\Delta^y = \Delta$. If $\delta, \delta^x \in \Theta_1$, then $\Delta = \Delta^H = \Omega$, a contradiction. Hence we may assume that $\beta, \gamma \in \Theta_1 \subseteq \Delta$ and so $\beta^x, \gamma^x \in \Delta^x$. Since $\beta^{xy} = \gamma^x$ it follows that $(\Delta^x)^y = \Delta^x$. Therefore $\Theta_3 \subseteq \Delta^x$ and so $|\Delta^x| = (m-1)k > \frac{n}{2}$, a contradiction.

Thus H is primitive and contains the p_k-cycle $y^{(m-1)k(k-p_k)} \in \mathcal{J}_c$. Hence $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y.

Now assume that $p_k p_k{}' \mid (m-1)$. Since $x \notin \mathcal{J}$, Lemma 6.4.4(i) and (ii) imply that there exist either $\alpha, \alpha^x \in \Omega_1$ or $\beta \in \Omega_1 \backslash \{1\}$ such that $\beta^x \notin \Omega_1 \cup \Omega_2$; there exist distinct points $\gamma, \gamma^x \in \mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega(\beta^x))$; and an element with cycle type $1^{n-p_m k} \cdot p_m^k$ is in $\mathcal{J}_w$. Observe that $p_m > k$ by the latter deduction.

By Lemma 4.2.1 an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega(\beta^x),\Omega(\gamma),\Omega(\gamma^x)\in\mathrm{Supp}((c_1,c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_3^{\mathcal{M}})=(m-p_m) \\ \Omega_2\in\mathrm{Supp}(c_3^{\mathcal{M}})}}$$

such that $1, 1^y = \gamma \in \Theta_1, \gamma^x \in \Theta_2$, $k+1 \in \Theta_3$ and either α, α^x or $\beta, \beta^x \in \Theta_1$. Then, $H = H(y) = \langle x, y \rangle$ is transitive.

We claim that there exists $y \in \mathcal{Y}$ for which H is primitive by Lemma 4.2.15. Let $(q_1, q_2, i, j, \upsilon, \phi) = (p_m, p_k, 3, 2, 1, \gamma)$ and either $\psi = \alpha = \omega$ or $\psi = \beta = \omega$. Then $p_m \nmid |\Theta_3|$ and $p_k \nmid |\Theta_2|$, hence $p_m p_k \nmid |\Theta_l|$ for $2 \leq l \leq 3$. Also $1, \gamma \in \Theta_1$, $1^x = k+1 \in \Theta_3$ and $\gamma^x \in \Theta_2$, and either $\alpha, \alpha^x \in \Theta_1$ or $\beta, \beta^x \in \Theta_1$. Finally $1^{\langle y^{p_m} \rangle} = \Omega_1 \cap \Theta_1$ contains either α or β, and by Lemma 4.2.13(iv) there exists $y \in \mathcal{Y}$ such that $\gamma^{\langle y^{p_k} \rangle}$ contains either α or β. Hence Conditions (i), (ii) and (iii)(a) of Lemma 4.2.15 are satisfied, and so the claim holds

Now $y^{p_k(k-p_k)(m-p_m)k}$ has cycle type $1^{n-p_m k} \cdot p_m^k$, and so $y^{p_k(k-p_k)(m-p_m)k} \in \mathcal{J}_w$. Hence $H = G$ by Theorem 4.3.4. □

We now complete the proof in the case of $x \notin \hat{M}$.

Lemma 6.4.6. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then the result holds by Lemma 6.4.5. Hence we may assume that $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, and so $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ since $x \in X_1$. If there exist $3 \leq i, j \leq m$ such that $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$, then the result holds by Lemma 6.4.2. Hence assume otherwise, and so by Proposition 6.2.6(iv) we may assume that there exists $\alpha \in \Omega_3 \cap \mathrm{Supp}(x)$, $\beta \in \Omega_5 \cap \mathrm{Supp}(x)$ and $i \in \{1, 4\}$ such that $\alpha^x \in \Omega_i$. If $p_k \nmid (m-2)$, then let $a := 2$, otherwise let $a := 4$. Thus $p_k \nmid (m-a)$ and $(m-a) > a, a-1$.

Since $k \geq 28$, there exists $\gamma_5 \in \Omega_5 \backslash \{\beta, \beta^{x^{-1}}\}$ and $\gamma_6 \in \Omega_6 \backslash \{\beta^{x^{-1}}\}$. From $\Omega_2 \cap \mathrm{Supp}(x) = \{k+1\} = \{1^x\}$ it follows that $\gamma_5^x, \gamma_6^x \notin \Omega_2$.

By Lemma 4.2.1 an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$.

Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(y) = \underbrace{ap_k \cdot a(k-p_k)}_{(l(c_1c_2)^{\mathcal{M}})=a} \cdot \underbrace{(m-a)k}_{l(c_3^{\mathcal{M}})=m-a}.$$

such that y satisfies all of the following.

(i) If $a = 2$ then $(c_1c_2)^{\mathcal{M}} = (\Omega_1, \Omega_5)$, and if $a = 4$ then $(c_1c_2)^{\mathcal{M}} = (\Omega_1, \Omega_5, \Omega_6, \Omega_7)$.

(ii) $1 \in \Theta_1, \beta \in \Theta_2$ and $\beta^x \in \Theta_1 \cup \Theta_3$.

(iii) If $a = 2$ then let $\gamma = \gamma_5 = 1^{y^{p_k}}$, and if $a = 4$ then let $\gamma = \gamma_6 = 1^{y^{2p_k}}$. Also $\gamma^x \in \Theta_1 \cup \{(k+1)^{y^i} \mid 1 \leq i < m-a\}$.

(iv) One of the follows holds.

  (a) If $\alpha^x \in \Omega_1$, then $(k+1)^{y^{-1}} = \alpha$.

  (b) If $\alpha^x \in \Omega_4$, then $(k+1)^{y^{-a}} = \alpha$ and $(k+1)^{y^{-(a+1)}} = \alpha^x$.

By Conditions (i) and (ii), $H = \langle x, y \rangle$ is transitive. Assume, by way of contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since Θ_1 contains points of $\Omega_1 \backslash \{1\} \subseteq \text{Fix}(x)$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$. Since $p_k \nmid |\Theta_2|, |\Theta_3|$, Lemma 4.2.14(ii) implies that $l(c_1^{\mathcal{H}}) \neq ap_k$.

If $a = 2$ then let $d = 1$, and if $a = 4$ then let $d \in \{1, 2\}$. Hence $d < a$ is a divisor of a. Assume that $l(c_1^{\mathcal{H}}) = dp_k$. Then by Condition (iii), $1, \gamma \in \Delta$. Since $p_k \nmid |\Theta_2|, |\Theta_3|$ it follows by Lemma 4.2.11(iv) that $\Delta \subseteq \Theta_1$ and so $|\Delta| = \frac{a}{d} \leq 4$. If $\gamma^x \in \Theta_1 \cup \Theta_2$, then $\gamma^x \in \Theta_1$ by Condition (iii), and so Δ^x contains $\gamma^x \in \Theta_1$ and $k+1 \in \Theta_3$. Hence $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$ by Lemma 4.2.11(i), a contradiction since $p_k \nmid |\Theta_3|$. If $\gamma^x \in \Theta_3$, then by Condition (iii), there exists $1 \leq i \leq m-a$ such that $(k+1)^{y^i} = \gamma^x$. Hence $(\Delta^x)^{y^i} = \Delta^x$, and so $|\Delta^x| \geq \frac{(m-a)k}{i} \geq k > 4 \geq |\Delta|$, a contradiction.

Let $e > 1$ be a divisor of a and assume that $l(c_1^{\mathcal{H}}) = e$. Then in particular $\Delta^{y^a} = \Delta$. By Lemma 4.2.13(ii) we deduce that $\Omega_1 \cap \Theta_1 \subseteq \Delta \cap \Theta_1$. Since $|\Omega_1 \cap \text{Supp}(x)| = 1$ it follows that $\Delta^x = \Delta$, and so $k+1 \in \Delta$. Recall that $\alpha^x \in \Omega_1 \cup \Omega_4$. If $\alpha^x \in \Omega_1$, then from $|\Omega_1 \cap \text{Supp}(x)| = 1$ it follows that $\alpha^x = 1 \in \Delta$. From $\Delta^x = \Delta$ and Condition (iv)(a), we deduce that $\alpha = (k+1)^{y^{-1}} \in \Delta$, and so $\Delta = \Delta^H = \Omega$, a contradiction. Hence $\alpha^x \in \Omega_4$. Since $\Delta^x = \Delta = \Delta^{y^a}$ and $k+1 \in \Delta$ it follows by Condition (iv)(b) that $\alpha = (k+1)^{y^{-a}}, \alpha^x = (k+1)^{y^{-a}x} \in \Delta$. Since $\alpha^{xy} = \alpha$, we deduce that $\Delta = \Delta^H = \Omega$, a contradiction.

Therefore H is primitive and contains $y^{a(m-a)k(k-p_k)}$ which has cycle type $1^{n-ap_k} \cdot {p_k}^a$.

We now show that this is a Jordan element. Now $a = 2$ or 4, $p_k \geq 7$ and

$$n - ap_k = mk - ap_k > (m - a)p_k > (m - 4)p_k > 4.$$

Hence $y^{a(m-a)k(k-p_k)} \in \mathcal{J}_w$, and so $H = G$ by Theorem 4.3.4. □

6.4.2 $\boldsymbol{x \in (X_1 \cap \hat{M})\backslash \mathcal{J}}$

In this subsection we prove Proposition 6.4.1 under the assumption that $x \in (X_1 \cap \hat{M})\backslash \mathcal{J}$.

We begin with the case of $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$. For $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ we first assume that $m \geq 4k - 2$, secondly that $k \leq m < 4k - 2$, and then we consider the general case. Finally we complete the proof of Proposition 6.4.1.

Lemma 6.4.7. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A). *If $x \in (X_1 \cap \hat{M})\backslash \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. We first show that there exist $\alpha \in (\Omega_1 \cap \mathrm{Supp}(x))\backslash\{1\}$ and $\beta, \beta^x \in \Omega_1\backslash\{\alpha\}$.

If $\Omega_1 \cap \mathrm{Fix}(x) \neq \emptyset$, then let $\beta = \beta^x \in \Omega_1 \cap \mathrm{Fix}(x)$ and let $\alpha \in \Omega_1 \cap \mathrm{Supp}(x)\backslash\{1\}$. Hence assume that $\Omega_1 \cap \mathrm{Fix}(x) = \emptyset$. Since $x \in \hat{M}$ it follows that $\Omega_1^x \subseteq \Omega_1 \cup \Omega_2$, and since $x \notin M$ it follows that $\Omega_1^x \neq \Omega_2$. Hence there exist $\beta, \beta^x \in \Omega_1$ and we may let $\alpha \in \Omega_1\backslash\{1, \beta, \beta^x\}$.

By Lemma 4.2.1 an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. We split into two cases. First assume that there exists a Bertrand prime p_k such that $p_k \nmid (m-1)$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_k \cdot (k - p_k)}_{\Theta_1 \cup \Theta_2 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_3^{\mathcal{M}}) = m-1},$$

such that $1, \beta, \beta^x \in \Theta_1$, $\alpha \in \Theta_2$, and $\alpha^x \in \Theta_1 \cup \Theta_3$. Then $H = \langle x, y\rangle$ is transitive. Assume, by way of contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Since $p_k \nmid |\Theta_2|, |\Theta_3|$, Lemma 4.2.14(ii) implies that $l(c_1^{\mathcal{H}}) \neq p_k$ and since $\beta, \beta^x \in \Theta_1$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$. Thus H is primitive and contains the p_k-cycle $y^{(k-p_k)(m-1)k} \in \mathcal{J}_c$. Therefore $H = G$ by Theorem 4.3.4.

If there is no p_k as in the previous case, then by Lemma 4.4.11 there exist a prime $q > p_k$ such that $q \nmid mk$, $k < (m - q)$ and $kq < 2(\sqrt{n} - 1)$. By Lemma 6.2.3 there exist $\gamma, \gamma^x \in \Omega_3$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{qp_k \cdot q(k - p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}}) = q \\ \Omega_1, \Omega_3 \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m - q)k}_{\substack{l(c_3^{\mathcal{M}}) = m-q \\ \Omega_2 \in \mathrm{Supp}(c_3^{\mathcal{M}})}}$$

with $1, \beta, \beta^x, \gamma, \gamma^x \in \Theta_1$, $\alpha \in \Theta_2$, and $\alpha^x \in \Theta_1 \cup \Theta_3$. Then $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H preserves a non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $\gamma, \gamma^x \in \Theta_1$ it follows by Lemma 4.2.14(i) that $l(c_1^{\mathcal{H}}) \neq 1$. Since $p_k \nmid q(k - p_k)$ and $q \nmid (m - q)k$, it follows by Lemma 4.2.14(ii) that $l(c_1^{\mathcal{H}}) \neq qp_k$.

Assume that $l(c_1^{\mathcal{H}}) = p_k$. Then Lemma 4.2.13(iv) implies that $|\Delta \cap \Omega_j \cap \Theta_1| = 1$ for each $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$. Hence there exists $y \in \mathcal{Y}$ such that $1, \gamma \in \Delta$. Therefore $k + 1, \gamma^x \in \Delta^x$ and so by Lemma 4.2.11(i) it follows that $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$. Hence by Lemma 4.2.10 $p_k \mid (m - q)k$. Since $p_k \nmid k$ it follows that $p_k \mid (m - q)$. Let Γ be an arbitrary block in $\mathrm{Supp}(c_3^{\mathcal{H}})$. From $m - q > k > p_k$, Lemma 4.2.13(ii) implies that $\Gamma \cap \Theta_3$ is a union of at least two M-blocks. Since $\Omega_j^x = \Omega_j$ for $j \neq 1, 2$, it follows that $\Gamma^x = \Gamma$. Hence from $\alpha^x \in \Theta_1 \cup \Theta_3$, $\alpha \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Assume finally that $l(c_1^{\mathcal{H}}) = q$. Then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i). Hence $\beta, \beta^x \in \Delta$, and so $\Delta^x = \Delta$ and $k + 1 \in \Delta \cap \Theta_3$. From $q \nmid |\Theta_3|$ we derive a contradiction by Lemma 4.2.14(iii).

Hence H is primitive. Since $q \nmid mk$ it follows that $y^{(m-q)k}$ is non-trivial and has support size $kq < 2(\sqrt{n} - 1)$. Therefore $y^{(m-q)k} \in \mathcal{J}_s$, and so $H = G$ by Theorem 4.3.4. □

For the rest of this section we may assume that $x \in \hat{M}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$. We split into three cases, first $m \geq 4k - 2$ then $k \leq m < 4k - 2$ and finally $m < k$.

We first prove a preliminary lemma which guarantees the existence of certain points.

Lemma 6.4.8. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A). *Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$,* $\mathrm{Supp}(x) \cap (\Omega_1 \cup \Omega_2) = \{1, k+1\}$ *and* $\mathrm{Supp}(x) \not\subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$ *for any $3 \leq i, j \leq m$. Then there exist distinct points $\alpha, \alpha^x \in \Omega_3 \cap \mathrm{Supp}(x)$, $\beta, \beta^x \in \Omega_4 \cap \mathrm{Supp}(x)$, $\gamma, \gamma^x \in \Omega_5 \cap \mathrm{Supp}(x)$ and $\delta, \delta^x, \epsilon, \epsilon^x \in (\Omega_5 \cup \Omega_6 \cup \Omega_7) \cap \mathrm{Supp}(x)$.*

Proof. By Proposition 6.2.6(iii) we may assume that

$$0 < |\Omega_3 \cap \mathrm{Supp}(x)| \leq |\Omega_4 \cap \mathrm{Supp}(x)| \leq |\Omega_5 \cap \mathrm{Supp}(x)|.$$

Hence there exists $\alpha, \alpha^x \in \Omega_3 \cap \mathrm{Supp}(x)$ and $\beta, \beta^x \in \Omega_4 \cap \mathrm{Supp}(x)$. If $|\Omega_5 \cap \mathrm{Supp}(x)| \geq 7$, then there exists $\gamma \in \Omega_5 \cap \mathrm{Supp}(x)$, $\delta \in \Omega_5 \cap \mathrm{Supp}(x) \backslash \{\gamma, \gamma^x, \gamma^{x^{-1}}\}$ and $\epsilon \in \Omega_5 \cap \mathrm{Supp}(x) \backslash \{\gamma, \gamma^x, \gamma^{x^{-1}}, \delta, \delta^x, \delta^{x^{-1}}\}$. Otherwise $|\Omega_5 \cap \mathrm{Supp}(x)| \leq 6$ and so $|\Omega_3 \cap \mathrm{Supp}(x)| \leq 6$ and $|\Omega_4 \cap \mathrm{Supp}(x)| \leq 6$. Since $x \notin \mathcal{J}_s$ it follows that $|\mathrm{Supp}(x)| > 2(\sqrt{19 \cdot 28} - 1) \geq 44$. Hence assume otherwise, and so

$$|\mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4)| \geq 44 - 2(1) - 2(6) = 30.$$

Therefore there exist distinct points $\gamma, \gamma^x, \delta, \delta^x, \epsilon, \epsilon^x \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4)$. Since $x \in \hat{M}$ these points lie in at most three M-blocks. Hence by Proposition 6.2.6(iii), we may assume that $\gamma, \gamma^x \in \Omega_5 \cap \mathrm{Supp}(x)$ and $\delta, \delta^x, \epsilon, \epsilon^x \in (\Omega_5 \cup \Omega_6 \cup \Omega_7) \cap \mathrm{Supp}(x)$. □

Lemma 6.4.9. *Let $k \geq 28$, let $m \geq 4k-2$, and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in (X_1 \cap \hat{M})\backslash\mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Lemma 4.4.18 since $m, k \geq 18$, there exist distinct primes p_m and p_k such that $\frac{m+5}{2} \leq p_m \leq m-5$ and $p_k \leq k-5$. Hence

$$p_m > \frac{m}{2} \geq 2k-1 > k-2, \tag{6.5}$$

and so p_m does not divide any of p_k, $(k-2)$ and $(k-p_k)$. From $x \in X_1$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. If $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$ for some i and j, then the result follows by Lemma 6.4.2. Since $x \notin \mathcal{J}$, we may let α, β, γ be as in Lemma 6.4.8.

By Lemma 4.2.1 an element composed of five cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4c_5 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m(k-2)\cdot p_m \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega_3,\Omega_5\in\mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{p_k(m-p_m)\cdot(k-p_k)(m-p_m)}_{\substack{l((c_4c_5)^{\mathcal{M}})=m-p_m \\ \Omega_2,\Omega_4\in\mathrm{Supp}((c_4c_5)^{\mathcal{M}})}}$$

with $1, 1^y = \gamma \in \Theta_1$, $\alpha, \gamma^x \in \Theta_2$, $\alpha^x \in \Theta_3$, $k+1, \beta \in \Theta_4$ and $\beta^x \in \Theta_5$. Hence $H = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H preserves a non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since Θ_1 contains points of $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$. From $p_m > m-p_m, p_k, k-p_k$ it follows that $(k-2)p_m \nmid |\Theta_i|$ for $i \neq 1$. Hence $l(c_1^{\mathcal{H}}) \neq (k-2)p_m$, by Lemma 4.2.14(ii).

Let $d < k-2$ be a divisor of $k-2$, and assume that $l(c_1^{\mathcal{H}}) = dp_m$. Then $|\Delta \cap \Omega_1 \cap \Theta_1| = \frac{(k-2)}{d} > 1$. Hence Δ contains a point of $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$, and so $\Delta^x = \Delta$. Since $k+1 \in \Theta_4$ and $dp_m \nmid |\Theta_4|$ we reach a contradiction by Lemma 4.2.14(iii).

Let $e > 1$ be a divisor of $k-2$, and assume that $l(c_1^{\mathcal{H}}) = e$. By Lemma 4.2.13(v), $|\Delta^y \cap \Omega_j| \geq 1$ for $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$. Hence Δ^y contains γ and a point of $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$. Therefore $\Delta^{yx} = \Delta^y$. Since $\gamma^x \in \Theta_2$ and $e \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Hence H is a primitive group. Let $t = (m-p_m)p_k(k-2)(k-p_k)$. Then $p_m \nmid t$, and so y^t has cycle type $1^{n-p_mk} \cdot p_m^k$. By assumption $k \geq 8$, and $p_m > 2k-1$ by (6.5), finally by

Lemma 4.4.18 $p_m + 4 \leq m$, and so

$$k(p_m + 4) - 4 \leq km - 4 < n.$$

Thus $y^t \in \mathcal{J}_w$ and so $H = G$ by Theorem 4.3.4. □

Lemma 6.4.10. *Let $k \geq 28$, let $k \leq m < 4k - 2$, and let G and M be as in Hypothesis 6.2.7*(A). *If $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Since $x \in X_1$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. If $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$ for some $3 \leq i, j \leq m$, then the result holds by Lemma 6.4.2. Hence we may let $\alpha, \beta, \gamma, \delta, \epsilon$ be as in Lemma 6.4.8. By Lemma 4.4.18 there exist distinct primes p_m and p_k such that $\frac{m+5}{2} \leq p_m \leq m - 5$, $p_k \leq k - 5$ and $p_k \nmid (m - 2)$.

First assume m is even. Hence $2 \nmid (m - p_m)$, and $G = \mathrm{S}_n$ by Hypothesis 6.2.7(A). We give two possibilities for $\mathcal{Y} \subseteq M$. By Lemma 4.2.1 an element composed of five or seven cycles is in $\mathrm{S}_n \backslash \mathrm{A}_n$. If k is even, then let $\mathcal{Y}$ be the set of elements $y = c_1 \cdots c_5 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k - p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}}) = p_m \\ \Omega_1, \Omega_4 \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m - p_m)(k - p_k - 2) \cdot (m - p_m)p_k \cdot (m - p_m)2}_{\substack{l((c_3c_4c_5)^{\mathcal{M}}) = m - p_m \\ \Omega_2, \Omega_3, \Omega_5 \in \mathrm{Supp}((c_3c_4c_5)^{\mathcal{M}})}}$$

with $1, 1^y = \beta \in \Theta_1$, $\beta^x \in \Theta_2$, $\alpha^x \in \Theta_3$, $k+1, \alpha, \gamma \in \Theta_4$, and $\gamma^x \in \Theta_5$. From $p_k \neq p_m$, we deduce that $p_k \nmid |\Theta_2|$ and $p_m \nmid |\Theta_4|, |\Theta_5|$. Since

$$p_m > \frac{m}{2} \geq \frac{k}{2} > k - p_k - 2 > k - p_k - 3, \tag{6.6}$$

it follows that $p_m \nmid |\Theta_3|$.

If k is odd, then let $\mathcal{Y}$ be the set of elements $y = c_1 \cdots c_7 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k - p_k - 1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}}) = p_m \\ \Omega_1, \Omega_3, \Omega_4 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m - p_m)p_k \cdot (m - p_m)(k - p_k - 3) \cdot (m - p_m) \cdot (m - p_m)2}_{\substack{l((c_4c_5c_6)^{\mathcal{M}}) = m - p_m \\ \Omega_2, \Omega_5, \Omega_6, \Omega_7 \in \mathrm{Supp}((c_4c_5c_6)^{\mathcal{M}})}}$$

with $1, 1^y = \beta, \alpha \in \Theta_1, \beta^x \in \Theta_2, \alpha^x \in \Theta_3$, $k+1, \gamma, \delta, \epsilon \in \Theta_4$ and $\gamma^x \in \Theta_5$, $\delta^x \in \Theta_6$ and $\epsilon^x \in \Theta_7$. Note that $p_k \nmid |\Theta_2|, |\Theta_3|$ and $p_m \nmid |\Theta_4|, |\Theta_6|, |\Theta_7|$. By (6.6), it follows that $p_m \nmid |\Theta_5|$.

In both cases, it is clear that H is transitive. We shall use Lemma 4.2.15 to show that H is primitive. Let $(q_1, q_2, i, j, \upsilon, \phi) = (p_m, p_k, 4, 2, 1, \beta)$. Then $p_m \nmid |\Theta_4|$, $p_k \nmid |\Theta_2|$ and $p_m p_k \nmid |\Theta_l|$ for $l \geq 2$. Also $1, \beta \in \Theta_1$, $1^x = k + 1 \in \Theta_4$ and $\beta^x \in \Theta_2$. Finally $1^y = \beta$

and by Lemma 4.2.13(i) $1^{\langle y^{p_m}\rangle} \subseteq \{1\} \cup \mathrm{Fix}(x)$. Hence Conditions (i), (ii) and (iii)(b) of Lemma 4.2.15 are satisfied, and so H is primitive.

If k is even then let $t = p_m p_k(k-p_k-2)(m-p_m)(k-p_k)$, and if k is odd then let $t = p_m p_k(k-p_k-1)(m-p_m)(k-p_k-3)$. Then y^t has cycle structure $1^{n-2(m-p_m)} \cdot 2^{m-p_m}$. From $p_m \geq \frac{m+5}{2}$, it follows that $-m-5 \geq -2p_m$, and so $m-5 \geq 2(m-p_m)$. In addition, $4k-2 > m$ implies that $k > \frac{m}{4} + \frac{1}{2} > \frac{m}{4}$, thus

$$2(\sqrt{n}-1) = 2(\sqrt{m}\sqrt{k}-1) > 2\Big(\sqrt{m}\sqrt{\frac{m}{4}}-1\Big) = m-2 > m-5 \geq 2(m-p_m).$$

Hence $y^t \in \mathcal{J}_s$, and so $H = G$ by Theorem 4.3.4.

Now suppose that m is odd. By Lemma 4.2.1 an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{2p_k \cdot 2(k-p_k)}_{(c_1c_2)^{\mathcal{M}}=(\Omega_1,\Omega_3)} \cdot \underbrace{(m-2)k}_{l(c_3^{\mathcal{M}})=m-2},$$

with $1, 1^y = \alpha \in \Theta_1$, $\alpha^x \in \Theta_2$ and $k+1 \in \Theta_3$. Hence $H = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$.

Since $p_k \nmid |\Theta_2|, |\Theta_3|$, it follows that $l(c_1^{\mathcal{H}}) \neq 2p_k$ by Lemma 4.2.14(ii). Since Θ_1 contains points of $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$ it follows that $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). Hence we may let Δ and $\Gamma := \Delta^y$ be distinct blocks with $1 \in \Delta$ and $\alpha \in \Gamma$.

Assume that $l(c_1^{\mathcal{H}}) = p_k$. Then, by Lemma 4.2.13(iv), $|\Gamma \cap \Omega_j \cap \Theta_1| = 1$ for $j = 1, 3$. In particular, Γ contains a point of $\Omega_1\backslash\{1\} \subseteq \mathrm{Fix}(x)$, and so $\Gamma^x = \Gamma$. Since $\alpha^x \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Assume that $l(c_1^{\mathcal{H}}) = 2$ so that $c_1^{\mathcal{H}} = (\Delta, \Gamma)$. Then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ and so $\Delta \cap \mathrm{Fix}(x) \neq \emptyset$. Hence $\Delta^x = \Delta$ and $1^x = k+1 \in \Delta$. Therefore $c_3^{\mathcal{H}} = (\Delta, \Gamma)$ by Lemma 4.2.11(i). From $m > 3$, we deduce that $mk > 3k$ and so $3mk - 3k > 2mk$. Hence $\frac{mk-k}{2} > \frac{mk}{3}$ and so

$$|\Delta| \geq p_k + \frac{(m-2)k}{2} > \frac{k}{2} + \frac{(m-2)k}{2} = \frac{(m-1)k}{2} > \frac{n}{3}.$$

Thus $\mathcal{H} = \{\Delta, \Gamma\}$. From $2 \nmid (m-2)$, it follows by Lemma 4.2.10 that $2 \mid k$. Hence $\Delta \cap \Omega_j \neq \emptyset$ and $\Gamma \cap \Omega_j \neq \emptyset$ for $\Omega_j \in \mathrm{Supp}(c_3^{\mathcal{M}})$ by Lemma 4.2.13(v). In particular, there exists $y \in \mathcal{Y}$ with $\beta \in \Delta$ and $\beta^x \in \Gamma$, contradicting the deduction that $\Delta^x = \Delta$.

Hence H is primitive and a power of y has cycle type $1^{n-2p_k} \cdot {p_k}^2$. Since $p_k \geq 5$ and $n - 2p_k > (m-2)p_k > 2$, it follows that $y^t \in \mathcal{J}_w$, and so $H = G$ by Theorem 4.3.4. □

Lemma 6.4.11. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $m \geq 4k-2$, then the result holds by Lemma 6.4.9 and if $k \leq m < 4k-2$, then the result holds by Lemma 6.4.10. Hence we may assume that $m < k$. Therefore by Lemma 4.4.19 since $m \geq 18$ there exist distinct primes p_m and p_k such that

$$p_k \neq m-3 \qquad m - p_m \geq 2 \quad \text{and} \quad k-2 > p_k > \frac{k}{2} > \frac{m}{2} > m - p_m. \tag{6.7}$$

Since $x \in X_1$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. If $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_i \cup \Omega_j$ for some $3 \leq i, j \leq m$, then the result holds by Lemma 6.4.2. Hence we may assume otherwise and let $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x$ be as in Lemma 6.4.8.

First assume that $3 \nmid (m - p_m)$. By Lemma 4.2.1 an element composed of five cycles lies in A_n if and only if $G = \mathrm{A}_n$. If $3 \nmid (k - p_k)$, then let $\mathcal{Y}$ be the set of elements $y = c_1 \cdots c_5 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}}) = p_m \\ \Omega_1, \Omega_3 \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)(k-p_k-3) \cdot (m-p_m)3 \cdot (m-p_m)p_k}_{\substack{l((c_3c_4c_5)^{\mathcal{M}}) = m-p_m \\ \Omega_2, \Omega_4, \Omega_5 \in \mathrm{Supp}((c_3c_4c_5)^{\mathcal{M}})}}$$

with $1, 1^y = \alpha \in \Theta_1$, $\alpha^x \in \Theta_2$, $\gamma^x \in \Theta_3$, $\beta^x \in \Theta_4$, and $k+1, \beta, \gamma \in \Theta_5$. Note that $p_k \nmid |\Theta_2|$ and $p_m \nmid |\Theta_4|, |\Theta_5|$, and by (6.7) $p_k \nmid |\Theta_3|$.

If $3 \mid (k - p_k)$, then $3 \nmid (k - p_k - 1)(k-3)$. Let $\mathcal{Y}$ be the set of elements $y = c_1 \ldots c_5 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k-1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}}) = p_m \\ \Omega_1, \Omega_3, \Omega_4 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)(k-3) \cdot (m-p_m)3}_{\substack{l((c_4c_5)^{\mathcal{M}}) = m-p_m \\ \Omega_2, \Omega_5 \in \mathrm{Supp}((c_4c_5)^{\mathcal{M}})}}$$

with $1, 1^y = \alpha, \beta \in \Theta_1, \alpha^x \in \Theta_2$, $\beta^x \in \Theta_3$, $\gamma^x \in \Theta_4$ and $k+1, \gamma \in \Theta_5$. Note that $p_k \nmid |\Theta_2|, |\Theta_3|$ and $p_m \nmid |\Theta_5|$. By (6.7), $p_k \neq k-3$ and $p_k > m - p_m$, and so $p_k \nmid |\Theta_4|$.

In both cases H is transitive. We shall use Lemma 4.2.15 to show that H is primitive. Let $(q_1, q_2, i, j, \upsilon, \phi) = (p_m, p_k, 5, 2, 1, \alpha)$. Then $p_m \nmid |\Theta_5|$, $p_k \nmid |\Theta_2|$ and $p_m p_k \nmid |\Theta_l|$ for $2 \leq l \leq 5$. Also, $1, \alpha \in \Theta_1$, $1^x = k+1 \in \Theta_5$ and $\alpha^x \in \Theta_2$. Finally $1^y = \alpha$ and by Lemma 4.2.13(i) $1^{\langle y^{p_m} \rangle} \subseteq \{1\} \cup \mathrm{Fix}(x)$. Hence H satisfies Conditions (i), (ii) and (iii)(b) of Lemma 4.2.15 and so H is primitive.

There exists a power of y with cycle type $1^{n-3(m-p_m)} \cdot 3^{(m-p_m)}$. Since $m > 2$ it follows that $4m - 2 > 3m$. Hence $2(m-1) > \frac{3m}{2}$, and so

$$2(\sqrt{n} - 1) > 2(m-1) > 3\Big(\frac{m}{2}\Big) > 3(m - p_m).$$

Therefore $y^t \in \mathcal{J}_s$ and so $H = G$ by Theorem 4.3.4.

Now assume that $3 \mid (m - p_m)$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{3p_k \cdot 3(k - p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}})=3 \\ \Omega_1,\Omega_3 \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-3)k}_{\substack{l(c_3^{\mathcal{M}})=m-3 \\ \Omega_2,\Omega_4 \in \mathrm{Supp}(c_3^{\mathcal{M}})}}$$

with $1, 1^y = \alpha \in \Theta_1$, $\alpha^x \in \Theta_2$ and $k+1, \beta, \beta^x \in \Theta_3$ and $(k+1)^{y^3} = \beta$. Hence $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H preserves a non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Clearly $p_k \nmid |\Theta_2|$. By (6.7) we have $p_k > \frac{m}{2} > \frac{m-3}{2}$ and $p_k \neq m - 3$, hence $p_k \nmid |\Theta_3|$. Therefore $l(c_1^{\mathcal{H}}) \neq 3p_k$ by Lemma 4.2.14(ii). Since Θ_1 contains points of $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$ it follows that $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i).

Assume that $l(c_1^{\mathcal{H}}) = p_k$. Then by Lemma 4.2.13(iv), $|\Delta^y \cap \Omega_j \cap \Theta_1| = 1$ for $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$. In particular, Δ^y contains α and a point of $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$. Hence $(\Delta^y)^x = \Delta^y$. Since $\alpha^x \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Now assume that $l(c_1^{\mathcal{H}}) = 3$. Then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i). Hence $\Delta^x = \Delta$ and $k + 1 \in \Delta$. Therefore $c_1^{\mathcal{H}} = c_3^{\mathcal{H}}$ by Lemma 4.2.11(i), and since $3 \nmid (m-3)$, Lemma 4.2.10 implies that $3 \mid k$. Hence $\Delta \cap \Omega_j \neq \emptyset$ for $\Omega_j \in \mathrm{Supp}(c_3^{\mathcal{M}})$ by Lemma 4.2.13(v). Therefore $\beta \in \Delta$, and there exists $y \in \mathcal{Y}$ such that $\beta^x \notin \Delta$. A contradiction since $\Delta^x = \Delta$.

Hence H is primitive and a power of y has cycle type $1^{n-3p_k} \cdot {p_k}^3$. Since $p_k \geq 5$, and $n - 3p_k > (m-3)p_k > 3$, it follows that $y^t \in \mathcal{J}_w$. Hence $H = G$ by Theorem 4.3.4. □

Proof of Proposition 6.4.1. By Proposition 6.2.8, we may assume that $x \in X_1$. If $x \notin \hat{M}$, then the result holds by Lemma 6.4.6. If $x \in \hat{M}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then the result holds by Lemma 6.4.7. If $x \in \hat{M}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then the result holds by Lemma 6.4.11. □

6.5 Hypothesis 6.2.7(B), Region four - $m \geq 19$ and $k \geq 28$

Here we prove the following lemma.

Proposition 6.5.1. *Let $m \geq 19$, let $k \geq 28$ and let G and M be as in Hypothesis 6.2.7*(B)*. Then for all $x \in X_1 \backslash \mathcal{J}$ there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Recall that X_1 is the set of elements $x \in G \backslash M$ such that $1^x = k + 1$, $\Omega_1^x \notin \mathcal{M}$ and

$|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$. In addition we recall the definition

$$\hat{M} = \mathrm{Sym}(\Omega_1 \cup \Omega_2) \times \Omega_3 \times \cdots \times \Omega_m.$$

We divide into two subsections, first that $x \in \hat{M}$ and then $x \notin \hat{M}$.

6.5.1 $\boldsymbol{x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}}$

In this subsection we assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$. We split into three cases: first we let $|\Omega_1 \cap \mathrm{Supp}(x)| > 3$; then let $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and assume that there exists $3 \leq i, j \leq m$ such that $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$; finally we assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and that $\mathrm{Supp}(x) \nsubseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for all $3 \leq i, j \leq m$.

$\boldsymbol{|\Omega_1 \cap \mathrm{Supp}(x)| > 3}$

Lemma 6.5.2. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *If $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| > 3$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. We begin by showing that there exist distinct points $\alpha, \beta \in \Omega_1 \backslash \{1\}$ such that $\beta^x \neq \alpha$, and points $\gamma, \gamma^x \in \Omega_1 \backslash \{\alpha, \beta\}$.

If $\Omega_1 \cap \mathrm{Fix}(x) \neq \emptyset$, then there exists $\gamma = \gamma^x \in \Omega_1 \cap \mathrm{Fix}(x)$. Since $|\Omega_1 \cap \mathrm{Supp}(x)| > 3$, there exist $\alpha \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$ and $\beta \in (\Omega_1 \cap \mathrm{Supp}(x)) \backslash \{1, \alpha, \alpha^x\}$.

Now assume that $\Omega_1 \subseteq \mathrm{Supp}(x)$. Since $x \in \hat{M}$ it follows that $(\Omega_1 \cup \Omega_2)^x = \Omega_1 \cup \Omega_2$, since $x \in X_1$ it follows that $\Omega_1^x \neq \Omega_2$. Therefore there exist $\gamma, \gamma^x \in \Omega_1 \cap \mathrm{Supp}(x)$. Now from $k \geq 6$ there exist $\alpha \in \Omega_1 \backslash \{1, \gamma, \gamma^x\}$ and $\beta \in \Omega_1 \backslash \{1, \gamma, \gamma^x, \alpha, \alpha^x\}$.

By Lemma 4.2.1 an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Using Lemma 4.4.11 we split into two cases. First assume that there exists a prime p_k such that $\frac{k}{2} < p_k < k-1$ and $p_k \nmid (m-1)$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{1 \cdot p_k \cdot (k - p_k - 1)}_{\Theta_1 \cup \Theta_2 \cup \Theta_3 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_4^{\mathcal{M}}) = m-1}$$

with $\Theta_1 = \{\alpha\}$, $1, \gamma, \gamma^x \in \Theta_2$, $\beta \in \Theta_3$, and $\beta^x \in \Theta_2 \cup \Theta_4$.

First note that since $\beta^x \neq \alpha$ it follows that $\mathcal{Y} \neq \emptyset$. Let $H = \langle x, y \rangle$. Then $1 \in \Theta_2$ and $k+1 \in \Theta_4$ imply that $\Theta_2 \cup \Theta_4 \subseteq 1^H$. Hence $\beta^x \in 1^H$, and so $\Theta_3 \in 1^H$. Therefore $\Omega \backslash \{\alpha\} \subseteq 1^H$, and since $\alpha \in \mathrm{Supp}(x)$ it follows that H is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Since $p_k \nmid |\Theta_i|$ for $i \neq 2$, Lemma 4.2.14(ii) implies that $l(c_2^{\mathcal{H}}) \neq p_k$. Since $\gamma, \gamma^x \in \Theta_2$ it follows that $l(c_2^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). Hence H is primitive by Lemma 4.2.10.

Since $y^{(k-p_k-1)(m-1)k}$ is a p_k-cycle it follows that $y^{(k-p_k-1)(m-1)k} \in \mathcal{J}_c$. Therefore $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y.

By Lemma 4.4.11, if there is no prime p_k as in the previous case, then there exist two primes $q > p_k$ such that $q \nmid mk$, $k < (m-q)$ and $kq < 2(\sqrt{n}-1)$. By Lemma 6.2.3 there exist $\lambda, \lambda^x \in \Omega_3$ (possibly equal). Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ with

$$\mathcal{C}(y) = \underbrace{qp_k \cdot q(k-p_k-1) \cdot q}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=q \\ \Omega_1,\Omega_3 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-q)k}_{\substack{l(c_4^{\mathcal{M}})=m-q \\ \Omega_2,\Omega_5 \in \mathrm{Supp}(c_4^{\mathcal{M}})}}$$

such that $1, \gamma, \gamma^x, \lambda, \lambda^x \in \Theta_1$, $\alpha \in \Theta_2$, $\beta \in \Theta_3$, $\beta^x \in \Omega_1 \cup \Omega_4$ and $\alpha^x \notin \Theta_2$. Hence $H = \langle x, y \rangle$ is transitive. We assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $p_k \nmid |\Theta_2|, |\Theta_3|$ and $q \nmid |\Theta_4|$, it follows that $l(c_1^{\mathcal{H}}) \neq qp_k$ by Lemma 4.2.14(ii). From $\gamma, \gamma^x \in \Theta_1$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$.

If $l(c_1^{\mathcal{H}}) = q$, then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i). Hence $\gamma, \gamma^x \in \Delta$ and so $\Delta^x = \Delta$. Since $k+1 \in \Theta_4$ and $q \nmid |\Theta_4|$ we reach a contradiction by Lemma 4.2.14(iii).

Suppose that $l(c_1^{\mathcal{H}}) = p_k$, so that there exist $\Delta_1 := \Delta, \Delta_2, \ldots, \Delta_{p_k} \in \mathcal{H}$ such that $c_1^{\mathcal{H}} = (\Delta_1, \ldots, \Delta_{p_k})$. By Lemma 4.2.13(iv), $|\Delta_i \cap \Omega_j \cap \Theta_1| = 1$ for $1 \leq i \leq p_k$ and $\Omega_j \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})$. Therefore there exists $y \in \mathcal{Y}$ such that $\lambda \in \Delta_1$. Since $\lambda^x \in \Theta_1$ it follows that $\Delta_1^x = \Delta_i$ for some $1 \leq i \leq p_k$. Therefore $k+1 \in \Delta_i$, and so $c_1^{\mathcal{H}} = c_4^{\mathcal{H}}$ by Lemma 4.2.11(i). Hence there exists $1 \leq l \leq p_k$ such that Δ_l containing β^x. Since $p_k \nmid k$ and $l(c_4^{\mathcal{H}}) = p_k$, we deduce by Lemma 4.2.10 that $p_k \mid (m-q)$. Therefore by Lemma 4.2.13(ii), there exists $\Omega_j \in \mathrm{Supp}(c_4^{\mathcal{M}})$ such that $\Omega_j \subseteq \Delta_l \cap \Theta_4$. By Lemma 6.2.3, $\Omega_j^x \cap \Omega_j \neq \emptyset$, and so $\Delta_l^x = \Delta_l$. However, $\beta \in \Theta_3$ and $p_k \nmid |\Theta_3|$ and so we reach a contradiction by Lemma 4.2.14(iii).

Therefore H is a primitive group containing $y_1 := y^{(m-q)k}$. From $q \nmid (m-q)k$, we deduce that $y_1 \neq \mathrm{id}$. In addition $|\mathrm{Supp}(y_1)| = qk < 2(\sqrt{n}-1)$, and so $y_1 \in \mathcal{J}_s$. Hence $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

$|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for any i, j

Here we assume that $x \in X_1$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$, and so $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$. We first assume further that $m \geq k$ before proving the general case. We begin with a technical lemma on the existence of certain points.

Lemma 6.5.3. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$, with $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $|\mathrm{Supp}(x)| \geq 36$, in addition*

$\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ *for any* i, j. *Then there exist distinct points* $\alpha, \alpha^x \in \Omega_5$, $\beta, \beta^x \in \Omega_5 \cup \Omega_6$, $\gamma, \gamma^x \in \Omega_5 \cup \Omega_6 \cup \Omega_7$, $\delta, \delta^x \in \Omega_5 \cup \Omega_6 \cup \Omega_7 \cup \Omega_8$, $\epsilon, \epsilon^x, \in \mathrm{Supp}(x) \cap \Omega_3$ *and* $\zeta, \zeta^x \in \mathrm{Supp}(x) \cap \Omega_4$*; and points* $\eta, \eta^x \in \Omega_3$, $\iota, \iota^x \in \Omega_4$ *and* $\kappa, \kappa^x \in \Omega_5$ *such that* $\eta, \eta^x, \iota, \iota^x, \kappa, \kappa^x \notin \{\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x, \epsilon, \epsilon^x, \zeta, \zeta^x\}$.

Proof. Since $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for all $3 \leq i, j \leq m$, Proposition 6.2.6(iii) implies that

$$0 < |\Omega_3 \cap \mathrm{Supp}(x)| \leq |\Omega_4 \cap \mathrm{Supp}(x)| \leq |\Omega_5 \cap \mathrm{Supp}(x)|.$$

Hence since $x \in \hat{M}$ there exist $\epsilon, \epsilon^x \in \Omega_3 \cap \mathrm{Supp}(x)$ and $\zeta, \zeta^x \in \Omega_4 \cap \mathrm{Supp}(x)$. If $|\Omega_5 \cap \mathrm{Supp}(x)| \geq 10$ then there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x \in \Omega_5 \cap \mathrm{Supp}(x)$. If $|\mathrm{Supp}(x) \cap \Omega_5| < 10$, then $|\mathrm{Supp}(x) \cap \Omega_3|, |\mathrm{Supp}(x) \cap \Omega_4| \leq 9$ and so

$$|\mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4)| \geq 36 - 2(3) - 2(9) = 12.$$

Therefore there exist distinct points $\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x \in \mathrm{Supp}(x) \backslash \{\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4\}$. Since $x \in \hat{M}$, these points lie in at most four M-blocks, and by Proposition 6.2.6(iii) we may assume that these four blocks are $\Omega_5, \Omega_6, \Omega_7, \Omega_8$.

Finally, since $x \in \hat{M}$ and $k \geq 28$, it is immediate that there exist $\eta, \eta^x \in \Omega_3$, $\iota, \iota^x \in \Omega_4$ and $\kappa, \kappa^x \in \Omega_5$ such that $\eta, \eta^x, \iota, \iota^x, \kappa, \kappa^x \notin \{\alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x, \epsilon, \epsilon^x, \zeta, \zeta^x\}$. □

First suppose that $m \geq k$.

Lemma 6.5.4. *Let* $k \geq 28$*, let* $m \geq k$ *and let* G *and* M *be as in Hypothesis 6.2.7*(B) *Assume that* $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ *with* $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ *and* $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ *for all* i, j*. Then there exists* $y \in M$ *such that* $\langle x, y \rangle = G$*.*

Proof. Since $35 < 2(\sqrt{n} - 1)$ and $x \notin \mathcal{J}_s$, we may assume that $|\mathrm{Supp}(x)| \geq 36$ and so there exists $\epsilon, \epsilon^x \in \Omega_3, \zeta, \zeta^x \in \Omega_4$ and $\alpha, \alpha^x, \beta, \beta^x \in \Omega_5 \cup \Omega_6$ as in Lemma 6.5.3.

First let $m \geq 4k - 2$. By Lemma 4.4.15 there exist distinct primes p_m and p_k, so that $p_m \neq p_k$ and $4 \leq m - p_m$. Since $m \geq 4k - 2$ it follows that $p_m > (k-2), (k - p_k - 1)$, and so in particular $p_m \nmid (k-2), (k - p_k - 1)$.

By Lemma 4.2.1 elements composed of six cycles are in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4c_5c_6 \in M$ such that

$$\mathcal{C}(y) = \underbrace{(k-2)p_m \cdot p_m \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega_5,\Omega_6 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{p_k(m-p_m) \cdot (m-p_m) \cdot (k-p_k-1)(m-p_m)}_{\substack{l((c_4c_5c_6)^{\mathcal{M}})=(m-p_m) \\ \Omega_2,\Omega_3,\Omega_4 \in \mathrm{Supp}((c_4c_5c_6)^{\mathcal{M}})}}$$

with $1, 1^y = \alpha, \beta \in \Theta_1, \alpha^x \in \Theta_2$, $\beta^x \in \Theta_3$, $k+1, \epsilon, \zeta \in \Theta_4, \epsilon^x \in \Theta_5$, $\zeta^x \in \Theta_6$, and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$. The final condition can be satisfied since $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$.

Hence $H = \langle x, y\rangle$ is transitive. Suppose, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$.

Suppose that $l(c_1^{\mathcal{H}}) = p_m$. Then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i), and so $\Delta^x = \Delta$ since $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Omega_2 \cup \Omega_3$. From $k+1 \in \Theta_4$ and $p_m \nmid |\Theta_4|$, we reach a contradiction by Lemma 4.2.14(iii).

Let d be a divisor of $k-2$, and assume that $l(c_1^{\mathcal{H}}) = d$ and let $\Sigma = \Delta^y$. Since $p_m > (k-2)$ it follows that $(d, p_m) = 1$. Then $|\Sigma \cap \Omega_j \cap \Theta_1| \geq 1$ for all $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$ by Lemma 4.2.13(v). Hence Σ contains α and a point of $(\Omega_1 \cap \Theta_1)\backslash\{1\} \subseteq \mathrm{Fix}(x)$. Therefore $\Sigma^x = \Sigma$ and so $\alpha^x \in \Sigma$. However $\alpha^x \in \Theta_2$ and $d \nmid p_m$, and so we reach a contradiction by Lemma 4.2.14(iii).

Let $e > 1$ be a divisor of $k-2$, and assume that $l(c_1^{\mathcal{H}}) = ep_m$, so that $|\Delta \cap \Theta_1| = \frac{k-2}{e}$. Since $dp_m \nmid |\Theta_i|$ for $i \neq 1$, Lemma 4.2.14(ii) implies that $|\Delta \cap \Theta_i| \neq \emptyset$ for $i \neq 1$. Hence $e < k-2$ since $\mathcal{H}$ is non-trivial. Therefore by Lemma 4.2.13(iii), Δ contains 1 and another point of $\Omega_1 \cap \Theta_1 \subseteq \mathrm{Fix}(x)$. Hence $\Delta^x = \Delta$ and $k+1 \in \Delta \cap \Theta_4$. Since $p_m \nmid |\Theta_4|$ we reach a contradiction by Lemma 4.2.14(iii).

Hence H is a primitive group. Let $y_1 = y^{p_k(m-p_m)(k-p_k-1)(k-2)}$. Then y_1 has cycle type $1^{n-p_mk} \cdot p_m^k$. Now $k \geq 8$ and $p_m > \frac{m}{2} \geq 2k-1$. By Lemma 4.4.15 $m - p_m \geq 4$, and so

$$n = mk \geq (p_m + 4)k > (p_m + 4)k - 4.$$

Hence $y_1 \in \mathcal{J}_w$ and so $H = G$ by Theorem 4.3.4.

Now suppose that $k \leq m < 4k-2$. By Lemmas 4.4.8, 4.4.15 and 4.4.16 there exist primes $p_m, p_k, {p_k}'$ and q such that $p_m \leq m-4$, $q \nmid m$, $p_k \nmid (m-q)$ and an element with cycle type $1^{n-p_kq} \cdot {p_k}^q$ is in $\mathcal{J}_w$. Hence by Definition 6.5 it follows that $q < p_k, {p_k}'$. Let $\epsilon, \epsilon^x \in \Omega_3$ and $\zeta, \zeta^x \in \Omega_4$ be as in Lemma 6.5.3. By Lemma 4.2.1, a product of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_kq \cdot (k-p_k)q}_{\substack{l((c_1c_2)^{\mathcal{M}})=q \\ \Omega_1,\Omega_3 \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{{p_k}'(m-q) \cdot (k-{p_k}')(m-q)}_{\substack{l((c_3c_4)^{\mathcal{M}})=m-q \\ \Omega_2,\Omega_4 \in \mathrm{Supp}((c_3c_4)^{\mathcal{M}})}}$$

with $1, 1^y = \epsilon \in \Theta_1$, $\epsilon^x \in \Theta_2$, $k+1, \zeta \in \Theta_3$, $\zeta^x \in \Theta_4$ and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2$.

Hence $H = \langle x, y\rangle$ is transitive. We claim that H is primitive by Lemma 4.2.15. Let $(q_1, q_2, i, j, \upsilon, \phi) = (q, p_k, 3, 2, 1, \epsilon)$. Then $q \nmid |\Theta_3|$, $p_k \nmid |\Theta_2|$ and $qp_k \nmid |\Theta_l|$ for $2 \leq l \leq 4$. Also $1, \epsilon \in \Theta_1$, $1^x = k+1 \in \Theta_3$ and $\epsilon^x \in \Theta_2$. Finally $1^y = \epsilon$ and $1^{\langle y^q\rangle} \subseteq \{1\} \cup \mathrm{Fix}(x)$. Hence H satisfies Conditions (i), (ii) and (iii)(b) of Lemma 4.2.15 and so is primitive.

Since $p_k \nmid |\Theta_l|$ for $l \neq 1$ it follows that the $(k-p_k)qp_k{}'(m-q)(k-p_k{}')^{th}$ power of y has cycle type $1^{n-p_k q} \cdot p_k{}^q$. Therefore $H = G$. □

We now consider the case of all m and k.

Lemma 6.5.5. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ with $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for any i, j. Then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $m \geq k$, then the result holds by Lemma 6.5.4. Hence we may assume that $m < k$. By Lemma 4.4.19 there exist distinct primes p_m and p_k such that $k - p_k \geq 5$ and $m - p_m \geq 5$. Since $x \notin \mathcal{J}_s$, we may assume that $|\mathrm{Supp}(x)| \geq 36$ and so Lemma 6.5.3 holds.

First assume that $3 \nmid (m - p_m)$. Let $\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \kappa$ be as in Lemma 6.5.3. Since $m > 4$ it follows that $3m < 4m - 4 = 4(m-1)$, and so $\frac{3m}{2} < 2(m-1)$. Hence since $p_m > \frac{m}{2}$ and $m < k$, we see that

$$3(m - p_m) < \frac{3m}{2} < 2(m-1) < 2(\sqrt{mk} - 1). \tag{6.8}$$

Hence an element with support $3(m-p_m)$ is in $\mathcal{J}_s$. By Lemma 4.2.1 an element composed of eight cycles is in A_n if and only if $G = \mathrm{A}_n$. We define two possibilities for $\mathcal{Y} \subseteq M$ and show that, in each case, if $y \in \mathcal{Y}$ then $\langle x, y \rangle$ is transitive and contains an element with support size $3(m - p_m)$.

If $3 \nmid (k - p_m)$, then $\mathcal{Y}$ be the set of elements $y = c_1 \cdots c_8 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k-3) \cdot p_m \cdot p_m \cdot p_m}_{\substack{l((c_1c_2c_3c_4c_5)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega_5,\Omega_6,\Omega_7,\Omega_8,\Omega_9 \in \mathrm{Supp}((c_1c_2c_3c_4c_5)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)p_k \cdot (m-p_m)(k-p_k-3) \cdot (m-p_m)3}_{\substack{l((c_6c_7c_8)^{\mathcal{M}})=m-p_m \\ \Omega_2,\Omega_3,\Omega_4 \in \mathrm{Supp}((c_6c_7c_8)^{\mathcal{M}})}}$$

with $1, 1^y = \alpha, \beta, \gamma, \delta, \kappa, \kappa^x \in \Theta_1$, $\alpha^x \in \Theta_2$, $\beta^x \in \Theta_3$, $\gamma^x \in \Theta_4$, $\delta^x \in \Theta_5$, $k+1, \epsilon, \zeta \in \Theta_6$, $\epsilon^x \in \Theta_7$, $\zeta^x \in \Theta_8$ and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$. Since $p_k \neq p_m$ it follows that $p_k \nmid |\Theta_2|, |\Theta_3|, |\Theta_4|, |\Theta_5|$ and $p_m \nmid |\Theta_6|, |\Theta_8|$. Furthermore, since $p_k > \frac{k}{2} > \frac{m}{2} > m - p_m$ it follows that $p_k \nmid |\Theta_7|$. Therefore the $p_m p_k (k - p_k - 3)(m - p_m)^{th}$ power of y has cycle type $1^{3(m-p_m)} \cdot 3^{(m-p_m)}$.

If $3 \mid (k - p_k)$, then $3 \nmid (k - p_k - 1)(k - p_k - 5)$. Let $\mathcal{Y}$ be the set of elements

$y = c_1 \cdots c_8 \in M$ such that

$$\begin{aligned}\mathcal{C}(y) = &\underbrace{p_m p_k \cdot p_m(k-p_k-1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1\Omega_3,\Omega_4 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \\ &\underbrace{(m-p_m)\cdot(m-p_m)\cdot(m-p_m)p_k\cdot(m-p_m)(k-p_k-5)\cdot(m-p_m)3}_{\substack{l((c_4c_5c_6c_7c_8)^{\mathcal{M}})=m-p_m \\ \Omega_1,\Omega_5,\Omega_6,\Omega_7,\Omega_8 \in \mathrm{Supp}((c_4c_5c_6c_7c_8)^{\mathcal{M}})}}\end{aligned}$$

with $1, 1^y = \epsilon, \zeta, \eta, \eta^x \in \Theta_1$, $\epsilon^x \in \Theta_2, \zeta^x \in \Theta_3$, $\alpha^x \in \Theta_4$, $\beta^x \in \Theta_5$, $k+1, \alpha, \beta, \gamma, \delta \in \Theta_6$, $\gamma^x \in \Theta_7$, $\delta^x \in \Theta_8$ and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$. Observe that, $p_k \nmid |\Theta_2|, |\Theta_3|$ and $p_m \nmid |\Theta_4|, |\Theta_5|, |\Theta_6|, |\Theta_8|$. Furthermore, since $p_k > \frac{k}{2} > \frac{m}{2} > m - p_m$ it follows that $p_k \nmid |\Theta_7|$. Therefore the $p_m p_k (k-p_k-1)(k-p_k-5)(m-p_m)^{th}$ power of y has cycle type $1^{3(m-p_m)} \cdot 3^{(m-p_m)}$.

Hence in both cases $H = \langle x, y \rangle$ is transitive. We claim that H is primitive by Lemma 4.2.15. Let $(q_1, q_2, i, j, \upsilon) = (p_m, p_k, 6, 2, 1)$, in addition: if $3 \nmid (k - p_k)$ then let $\phi = \alpha$; and if $3 \mid (k - p_k)$ then let $\phi = \epsilon$. Then $p_m \nmid |\Theta_6|$, $p_k \nmid |\Theta_2|$ and $p_m p_k \nmid |\Theta_l|$ for $2 \leq l \leq 8$. Also, $1, \phi \in \Theta_1$, $1^x = k+1 \in \Theta_6$ and $\phi^x \in \Theta_2$. Finally $1^y = \phi$ and $1^{\langle y^{p_m} \rangle} \subseteq \{1\} \cup \mathrm{Fix}(x)$. Hence H satisfies Conditions (i), (ii) and (iii)(b) of Lemma 4.2.15, and so H is primitive.

Thus in both cases, H is primitive and contains an element of $\mathcal{J}_s$. Therefore $H = G$ by Theorem 4.3.4, and so the result holds if $3 \nmid (m - p_m)$.

Now assume that $3 \mid (m - p_m)$. Let $\alpha, \epsilon, \zeta, \eta, \iota$ be as in Lemma 6.5.3. By Lemma 4.2.1 an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{3p_k \cdot 3 \cdot 3(k-p_k-1)}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=3 \\ \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})=\{\Omega_1,\Omega_3,\Omega_4\}}} \cdot \underbrace{(m-3)k}_{l(c_4^{\mathcal{M}})=m-3}$$

with $1, 1^y = \epsilon, \zeta, \eta, \eta^x, \iota, \iota^x \in \Theta_1$, $\epsilon^x \in \Theta_2$, $\zeta^x \in \Theta_3$, $k+1 \in \Theta_4$ and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$.

Hence $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $\eta, \eta^x \in \Theta_1$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$. By Lemma 4.4.19 $p_k \neq m - 3$ and combining this with $p_k > \frac{k}{2} > \frac{m}{2} > \frac{m-3}{2}$ gives $p_k \nmid |\Theta_4|$. Hence $p_k \nmid |\Theta_i|$ for $i \neq 1$, and so $l(c_1^{\mathcal{H}}) \neq 3p_k$ by Lemma 4.2.14(ii).

Assume that $l(c_1^{\mathcal{H}}) = p_k$. Then $|\Delta^y \cap \Omega_j \cap \Theta_1| = 1$ for all $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{H}})$ by Lemma 4.2.13(iv). Hence Δ^y contains ϵ and a point of $\Omega_1 \cap \mathrm{Fix}(x)$. Therefore $(\Delta^y)^x = \Delta^y$. Since

$\epsilon^x \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Hence we may assume that $l(c_1^{\mathcal{H}}) = 3$, so that there exist $\Delta_1 := \Delta, \Delta_2, \Delta_3 \in \mathcal{H}$ such that $c_1^{\mathcal{H}} = (\Delta_1, \Delta_2, \Delta_3)$. Then $\Delta_1 \cap \Theta_1 = \Omega_1 \cap \Theta_1$, $\Delta_2 \cap \Theta_1 = \Omega_3 \cap \Theta_1$ and $\Delta_3 \cap \Theta_1 = \Omega_4 \cap \Theta_1$ by Lemma 4.2.13(i), and so $\Delta_1 \cap \mathrm{Fix}(x) \neq \emptyset$, $\eta, \eta^x \in \Delta_2$ and $\iota, \iota^x \in \Delta_3$. Therefore Δ_1, Δ_2 and Δ_3 are fixed by x. Hence $k+1 \in \Delta_1$ and so $c_4^{\mathcal{H}} = (\Delta_1, \Delta_2, \Delta_3)$ by Lemma 4.2.11(i). From $3 \mid (m - p_m)$ we deduce that $3 \nmid (m-3)$, so by Lemma 4.2.10 we conclude that $3 \mid k$. Thus by Lemma 4.2.13(v), $1 \leq |\Delta_i \cap \Omega_j| < k$ for $1 \leq i \leq 3$ and $\Omega_j \in \mathrm{Supp}(c_4^{\mathcal{M}})$. Therefore there exists $y \in \mathcal{Y}$ and $1 \leq i \leq 3$, such that $\alpha \in \Delta_i$ and $\alpha^x \notin \Delta_i$. A contradiction since $\Delta_i^x = \Delta_i$.

Hence H is a primitive group containing the $3(k - p_k - 1)(m-3)k^{th}$ power of y which has cycle type $1^{n-3p_k} \cdot {p_k}^3$. Since $p_k \geq 5$ and $n - 3p_k > (m-3)p_k > 3$, this power of y is in $\mathcal{J}_w$. Hence $H = G$ by Theorem 4.3.4. □

$|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$

Here we assume that $x \in X_1$. Hence by Proposition 6.2.6(ii) we may assume $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$ and $|\Omega_3 \cap \mathrm{Supp}(x)| \geq |\Omega_4 \cap \mathrm{Supp}(x)|$.

This result comprises of three main lemmas: under the existence of certain primes we consider $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_3$ and $\mathrm{Supp}(x) \not\subseteq \{1, k+1\} \cup \Omega_3$ separately and then finally we prove the general case for this section. We begin with a preliminary lemma.

Lemma 6.5.6. *Let $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$, let $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and let $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$. If $|\mathrm{Supp}(x)| > 12$, then there exist distinct points $\alpha, \alpha^x, \beta, \beta^x \in \Omega_3$.*

Proof. Since $x \in X_1$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$, and so

$$|\mathrm{Supp}(x) \cap (\Omega_3 \cup \Omega_4)| \geq 12 - 2(3) = 6.$$

Therefore it follows that $|\Omega_3 \cap \mathrm{Supp}(x)| \geq 4$. Since $x \in \hat{M}$ it follows there exist $\alpha, \alpha^x, \beta, \beta^x \in \Omega_3 \cap \mathrm{Supp}(x)$. □

The next two lemmas assume that there exists primes q and p_k such that

$$q < \frac{m}{4}, \quad q \nmid m, \quad m - q \notin \{p_k, 2p_k\} \quad \text{and} \quad \frac{k+9}{2} \leq p_k \leq k-4. \tag{6.9}$$

Lemma 6.5.7. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B)*. Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ and $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_3$. If there exists primes q and p_k as in* (6.9)*, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Since $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_3$ it follows that $|\mathrm{Supp}(x)| \leq k+2$. If $k+9 \leq 4m$, then

$$\frac{(k+4)^2}{k} = k + 8 + \frac{16}{k} \leq 4m,$$

and so $k+4 \leq 2\sqrt{mk}$. Hence $|\mathrm{Supp}(x)| \leq k+2 \leq 2(\sqrt{mk}-1)$. Thus if either $k+9 \leq 4m$ or $|\mathrm{Supp}(x)| \leq 12$, then $x \in \mathcal{J}_s$, contradicting our assumptions on x. Hence assume otherwise and so we may let α be as in Lemma 6.5.6, and by (6.9)

$$p_k \geq \frac{k+9}{2} > 2m > 2m-1. \tag{6.10}$$

By Lemma 4.2.1 an element composed of two cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_k m \cdot (k-p_k)m}_{l((c_1c_2)^{\mathcal{M}})=m}$$

with $1, 1^y = k+1, 1^{y^2} = \alpha \in \Theta_1$ and $\alpha^x \in \Theta_2$. Hence $H = H(y) = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is primitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

By (6.10), $p_k \nmid m$. Hence $p_k \nmid |\Theta_2|$ and so $l(c_1^{\mathcal{H}}) \neq mp_k$ by Lemma 4.2.14(ii).

Since Θ_1 contains points of $\Omega_4 \subseteq \mathrm{Fix}(x)$ it follows that $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). Hence $\Delta^y \neq \Delta$, and so $k+1 \notin \Delta$.

Suppose that $l(c_1^{\mathcal{H}}) = p_k$ and let $\Gamma \in \mathcal{H}$ contain α. Then $\Gamma \cap \Omega_j \cap \Theta_1 \neq \emptyset$ for $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$ by Lemma 4.2.13(iv). In particular, Γ contains a point of $\Omega_4 \subseteq \mathrm{Fix}(x)$, and so $\Gamma^x = \Gamma$. Since $\alpha^x \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Let $d > 1$ be a divisor of m, and assume that $l(c_1^{\mathcal{H}}) = d$. Then $\Omega_1 \cap \Theta_1 \subseteq \Delta$ by Lemma 4.2.13(ii), and so $\Delta^x = \Delta$ since $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$. Hence $k+1 \in \Delta$, a contradiction.

Let $1 < e < m$ be a divisor of m, and assume that $l(c_1^{\mathcal{H}}) = p_k e$. Since $p_k \nmid |\Theta_2|$ it follows that $\Delta \subseteq \Theta_1$. Let $\beta \in \Delta \backslash \{1\}$. If $\beta \in \mathrm{Fix}(x)$, then $\Delta^x = \Delta$ and $k+1 \in \Delta$, a contradiction. Thus $\Delta \subseteq \mathrm{Supp}(x) \backslash \{k+1\} \subseteq \{1\} \cup \Omega_3$ and so $\beta \in \Omega_3$. By Lemma 4.2.13(vi) it follows that $\Delta = \{1, \beta\}$. Since $1^x = k+1 = 1^y$ it follows that $\Delta^x = \Delta^y$. However there exists $y \in \mathcal{Y}$ such that $\beta^y \neq \beta^x$, a contradiction.

Hence H is a primitive group containing $y^{m(k-p_k)}$ with cycle type $1^{n-mp_k} \cdot {p_k}^m$. Now by (6.9) and (6.10) it follows that

$$p_k \geq \frac{k+9}{2} \geq \frac{4m}{2} > 2m-1 \ \text{ and } \ n = mk > (p_k+4)m - 4.$$

Hence $y^{m(k-p_k)} \in \mathcal{J}_w$, and so $H = G$ by Theorem 4.3.4. □

Lemma 6.5.8. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B)*. Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ with $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$. If there exists primes q and p_k as in* (6.9)*, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $\mathrm{Supp}(x) \subseteq \{1, k+1\} \cup \Omega_3$ then the result holds by Lemma 6.5.7. Hence suppose that $\mathrm{Supp}(x) \not\subseteq \{1, k+1\} \cup \Omega_3$. Since $x \in X_1$ it follows that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$, hence we may assume that there exist either $\gamma, \gamma^x \in \Omega_4 \cap \mathrm{Supp}(x)$ or $\delta \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$. Since $x \in \hat{M}$, in the latter case $\delta^x \in \Omega_1 \cup \Omega_2$. Since $x \notin \mathcal{J}_s$ we may assume that $|\mathrm{Supp}(x)| > 12$, and let α and β be as in Lemma 6.5.6.

If $k + 9 \leq m$, then
$$\frac{(k+4)^2}{k} = k + 8 + \frac{16}{k} \leq k + 9 \leq m,$$
and so $k + 4 \leq \sqrt{mk}$. Hence $2k + 6 \leq 2(\sqrt{mk} - 1)$. Since $x \in X_1$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$, it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$. Thus from $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$ we deduce that $|\mathrm{Supp}(x)| \leq 2k + 6$. Hence if $k + 9 \leq m$, then $x \in \mathcal{J}_s$. Therefore we may assume that $k + 9 > m$.

By Lemma 4.2.1, elements composed of 4 cycles are in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ with

$$\mathcal{C}(y) = \underbrace{k(m-q)}_{\substack{l(c_1^{\mathcal{M}})=m-q \\ \Omega_1,\Omega_4 \in \mathrm{Supp}(c_1^{\mathcal{M}})}} \cdot \underbrace{p_kq \cdot (k-p_k-1)q \cdot q}_{\substack{l((c_2c_3c_4)^{\mathcal{M}})=q \\ \Omega_2,\Omega_3,\Omega_5 \in \mathrm{Supp}((c_2c_3c_4)^{\mathcal{M}})}}$$

such that $k+1, \alpha = (k+1)^y$, $\beta \in \Theta_2$, $\alpha^x \in \Theta_3$, $\beta^x \in \Theta_4$ and $(\mathrm{Supp}(x) \cap \Omega_2) \backslash \{k+1\} \subseteq \Theta_3$. Hence $H = \langle x, y \rangle$ is transitive. We assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $k + 1 \in \Delta$.

Since $(\mathrm{Supp}(x) \cap \Omega_2) \backslash \{k+1\} \subseteq \Theta_3$, Lemma 4.2.14(i) implies that $l(c_2^{\mathcal{H}}) \neq 1$. By (6.9) $q < \frac{m}{2} < \frac{k+9}{2} < p_k$, and so $p_k \nmid |\Theta_3|, |\Theta_4|$. Also by (6.9), $p_k \neq m - q$, and since

$$m - q < m < k + 9 \leq 2p_k$$

it follows that $p_k \nmid |\Theta_1|$. Hence Lemma 4.2.14(ii) implies that $l(c_2^{\mathcal{H}}) \neq p_kq$.

First assume that $l(c_2^{\mathcal{H}}) = p_k$. Then by Lemma 4.2.13(iv), $|\Delta^y \cap \Omega_j \cap \Theta_2| \geq 1$ for each $\Omega_j \in \mathrm{Supp}(c_2^{\mathcal{M}})$. In particular, Δ^y contains α and a point of $\Omega_5 \subseteq \mathrm{Fix}(x)$. Hence $(\Delta^y)^x = \Delta^y$ and so $\alpha^x \in \Delta^y$. Since $\alpha^x \in \Theta_3$ and $p_k \nmid |\Theta_3|$ we reach a contradiction by Lemma 4.2.14(iii).

Now assume that $l(c_2^{\mathcal{H}}) = q$, and let Γ be an arbitrary element of $\mathrm{Supp}(c_2^{\mathcal{H}})$. Then by Lemma 4.2.13(i) there exists $\Omega_j \in \mathrm{Supp}(c_2^{\mathcal{M}})$ such that $\Gamma \cap \Theta_2 = \Omega_j \cap \Theta_2$. Since $x \in \hat{M}$ and $(\mathrm{Supp}(x) \cap \Omega_2) \backslash \{k+1\} \subseteq \Theta_3$ it follows that $\Omega_j^x \cap \Omega_j \cap \Theta_2 \neq \emptyset$, and so $\Gamma^x = \Gamma$. Hence

$1 = (k+1)^{x^{-1}} \in \Delta$ and so $c_1^{\mathcal{H}} = c_2^{\mathcal{H}}$ by Lemma 4.2.11(i). Since $q \nmid m$ by (6.9), it follows that $q \mid k$ by Lemma 4.2.10. Hence Lemma 4.2.13 implies that $|\Gamma \cap \Omega_l \cap \Theta_1| = \frac{k}{q} < k$ for each $\Omega_l \in \mathrm{Supp}(c_1^{\mathcal{M}})$. Therefore there exists $y \in \mathcal{Y}$ and $\Gamma \in \mathrm{Supp}(c_2^{\mathcal{H}})$ such that either $|\Gamma \cap \{\gamma, \gamma^x\}| = 1$ or $|\Gamma \cap \{\delta, \delta^x\}| = 1$, contradicting the deduction that $\Gamma^x = \Gamma$.

Hence H is a primitive group containing $y^{k(m-q)q(k-p_k-1)}$, an element with cycle type $1^{n-p_kq} \cdot {p_k}^q$. From (6.9) and $m < k+9$, we deduce that

$$2q - 1 < 2q < 2\Big(\frac{m}{4}\Big) \le \frac{k+9}{2} \le p_k,$$

and

$$(p_k + 4)q - 4 < \frac{km}{4} - 4 < n.$$

Thus an element with cycle type $1^{n-p_kq} \cdot {p_k}^q$ is in $\mathcal{J}_w$. Therefore $H = G$ by Theorem 4.3.4. □

In the previous two lemmas we assumed the existence of primes p_k and q satisfying (6.9). Here we drop this assumption, and so complete the case of $x \in \hat{M}$, $|\Omega_1 \cap \mathrm{Supp}(x)| \le 3$ and $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$.

Lemma 6.5.9. *Let $m \ge 19$, let $k \ge 28$, and let G and M be as in Hypothesis 6.2.7*(B). *Assume that $x \in (X_1 \cap \hat{M}) \backslash \mathcal{J}$ with $|\Omega_1 \cap \mathrm{Supp}(x)| \le 3$ and $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$. Then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If there exists primes p_k and q as in (6.9), then the result holds by Lemmas 6.5.8 and 6.5.7. If $k \ge 33$; or if $28 \le k \le 32$, $19 \le m \le 41$ and $m \neq 30$ then Lemma 4.4.14 implies the existence of primes as in (6.9).

We show that if $m \ge 41$ and $28 \le k \le 32$, then $x \in \mathcal{J}$. First

$$\frac{(k+4)^2}{k} = k + 8 + \frac{16}{k} < k + 8 + 1 \le 41 \le m,$$

and so $k + 4 \le \sqrt{mk}$ and $2k + 6 \le 2(\sqrt{mk} - 1)$. Since $x \in X_1$, it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| \le 3$, and so $|\mathrm{Supp}(x)| \le 2k + 6$. Therefore if $m \ge 41$ then $x \in \mathcal{J}_s$.

Therefore we may assume that $m = 30$ and $28 \le k \le 32$. Since $x \notin \mathcal{J}$ it follows that $|\mathrm{Supp}(x)| > 12$, and so we may let α, β be as in Lemma 6.5.6. It can be verified in Magma (see Appendix - Lemma 8.1.1) that there exist distinct odd primes q_m, q_k and positive integers a, b such that $q_k + a + b = k$, $q_m < m$, $q_m \nmid mk$, $q_k \nmid ab(m - q_m)k$, and an element with cycle type $1^{n-q_kq_m} \cdot q_k^{q_m}$ is in $\mathcal{J}_s \cup \mathcal{J}_w$.

By Lemma 4.2.1 an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ to be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{q_m q_k \cdot q_m a \cdot q_m b}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=q_m \\ \Omega_1,\Omega_3,\Omega_5 \in \mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m - q_m)k}_{\substack{l(c_4^{\mathcal{H}})=m-p_m \\ \Omega_2 \in \mathrm{Supp}(c_4^{\mathcal{H}})}}$$

with $1, 1^y = \alpha \in \Theta_1$, $\alpha^x, \beta \in \Theta_2$, $\beta^x \in \Theta_3$ and $\Omega_1 \cap \mathrm{Supp}(x) \subseteq \{1\} \cup \Theta_2 \cup \Theta_3$.

Hence, $H = H(y) = \langle x, y \rangle$ is transitive. We claim that Lemma 4.2.15 implies that H is primitive. Let $(q_1, q_2, i, j, \upsilon, \phi) = (q_m, q_k, 4, 2, 1, \alpha)$. Then $q_m \nmid |\Theta_4|$, $q_k \nmid |\Theta_2|$ and $q_m q_k \nmid |\Theta_l|$ for $2 \leq l \leq 4$. Also $1, \alpha \in \Theta_1$, $1^x = k + 1 \in \Theta_4$ and $\alpha^x \in \Theta_2$. Finally $1^y = \alpha$ and $1^{\langle y^{q_m} \rangle} \subseteq \{1\} \cup \mathrm{Fix}(x)$. Hence H satisfies Conditions (i), (ii), and (iii)(b) of Lemma 4.2.15, and so H is primitive.

Hence H is primitive and contains $y_1 := y^{q_m ab(m-q_m)k}$, an element with cycle type $1^{n-q_k q_m} \cdot q_k^{q_m}$. By assumption on q_m and q_k, it follows that $y_1 \in \mathcal{J}_s \cup \mathcal{J}_w$. Hence $H = G$ by Theorem 4.3.4. □

6.5.2 $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$

We split into two cases based on $|\Omega_1 \cap \mathrm{Supp}(x)|$.

$|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$

We first assume the existence of certain primes, and then prove the general case.

Lemma 6.5.10. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B)*. Assume $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$ with $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$. If there exist distinct primes $p_k, p_k{}'$ such that $p_k \nmid (m-1)$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. We begin by proving the existence of certain points. Since $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$ there exists $\alpha \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$. By Proposition 6.2.6, we may assume that there exists $\beta \in \Omega_3$ such that $\beta^x \notin \Omega_3$. Since $x \notin \mathcal{J}_s$ we may assume that $|\mathrm{Supp}(x)| \geq 10$, and so there exists γ in $\mathrm{Supp}(x) \backslash \{1, k+1, 1^{x^{-1}}, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}\}$ so that $\gamma, \gamma^x \in \{1, k+1, \alpha, \alpha^x, \beta, \beta^x\}$.

Since $k \geq 28$, either there exists points $\delta, \delta^x \in \Omega_1 \backslash \{1, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}\}$, or distinct point $\epsilon, \zeta \in \Omega_1 \backslash \{1, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}\}$ such that $\epsilon^x, \zeta^x \notin \Omega_1$. By interchanging ϵ and ζ if necessary, we may assume that either $\epsilon^x \notin \Omega_2$ or $\epsilon^x, \zeta^x \in \Omega_2$.

By Lemma 4.2.1 elements composed of four cycles are in A_n if and only if $G = \mathrm{A}_n$. Let

$\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_k \cdot (k - p_k)}_{\Theta_1 \cup \Theta_2 = \Omega_1} \cdot \underbrace{(m-1){p_k}' \cdot (m-1)(k - {p_k}')}_{l((c_3c_4)^{\mathcal{M}}) = m-1}$$

satisfying the following.

(i) $1 \in \Theta_1$, $\alpha \in \Theta_2$, $k+1 \in \Theta_3$, $\beta \in \Theta_4$, $\alpha^x \notin \Theta_2$ and $\beta^x \notin \Theta_4$.

(ii) One of the following holds.

(a) If (α, β) is a not a cycle of x, then either $\beta^x \in \Theta_1 \cup \Theta_3$ or $\alpha^x \in \Theta_1 \cup \Theta_3$.

(b) If (α, β) is a cycle of x and $\gamma, \gamma^x \in \Omega_1$, then $\gamma \in \Theta_1$ and $\gamma^x \in \Theta_2$.

(c) If (α, β) is a cycle of x and $\gamma, \gamma^x \notin \Omega_1$, then $\gamma \in \Theta_3$ and $\gamma^x \in \Theta_4$.

(d) If (α, β) is a cycle of x and $|\Omega_1 \cap \{\gamma, \gamma^x\}| = 1$, then $\{\Theta(\gamma), \Theta(\gamma^x)\} = \{\Theta_2, \Theta_3\}$.

(iii) One of the following holds.

(a) If there exist $\delta, \delta^x \in \Omega_1$, then $\delta, \delta^x \in \Theta_1$.

(b) If there exist ϵ, ζ such that $\epsilon^x \notin \Omega_2$, then let $\epsilon, \zeta \in \Theta_1$, $(k+1)^y = \epsilon^x$ and $\zeta^x \in \Theta_4$.

(c) If there exist $\epsilon, \zeta \in \Omega_2$, then let $\epsilon, \zeta \in \Theta_1$, $\epsilon^x = (k+1)^{y^{(m-1)}}$ and $\zeta^x \in \Theta_4$.

We claim that $H = H(y) = \langle x, y \rangle$ is transitive. By Condition (i) it follows that $\Theta_1 \cup \Theta_3 \subseteq 1^H$. If (α, β) is not a cycle of x then by Condition (ii)(a) either α^x or $\beta^x \in \Theta_1 \cup \Theta_3 \subseteq 1^H$. If $\alpha^x \in 1^H$ then α, and so Θ_2 also, is in 1^H. Hence $\Omega \backslash \Theta_4 \subseteq 1^H$. Since $\beta \in \Theta_4$ and $\beta^x \notin \Theta_4$, it follows that $1^H = \Omega$. If $\beta^x \in 1^H$, then the argument above with α and β exchanged shows that H is transitive. Hence assume that (α, β) is a cycle of x. Then by Condition (i) $\Theta_1 \cup \Theta_3 \subseteq 1^H$ and $\Theta_2 \cup \Theta_4 \subseteq \alpha^H$. By Conditions (ii)(b)-(d), it follows that both of $\Theta_1 \cup \Theta_3$ and $\Theta_2 \cup \Theta_4$ contain exactly on point of $\{\gamma, \gamma^x\}$. Hence H is transitive.

Let $Y = \langle y \rangle$. Assume, by way of a contradiction, that H is an imprimitive group preserving a non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $p_k \nmid |\Theta_i|$ for $i \neq 1$, it follows $l(c_1^{\mathcal{H}}) \neq p_k$ by Lemma 4.2.14(ii). Hence $l(c_1^{\mathcal{H}}) = 1$ and $\Delta^y = \Delta$. If $\delta, \delta^x \in \Omega_1$, then $\Delta^x = \Delta$ by Condition (iii)(a), and so $\Delta = \Delta^H = \Omega$, a contradiction. Hence we may assume that $1, \epsilon, \zeta \in \Delta$ and $k+1, \epsilon^x, \zeta^x \in \Delta^x$. If $\epsilon^x \notin \Omega_2$, then $(\Delta^x)^y = \Delta^x$ by Condition (iii)(b). Hence $(k+1)^Y \cup (\zeta^x)^Y = \Theta_3 \cup \Theta_4 \subseteq \Delta^x$, and so $|\Delta^x| \geq (m-1)k > \frac{n}{2}$, a contradiction. If $\epsilon^x, \zeta^x \in \Omega_2$, then $(\Delta^x)^{y^{(m-1)}} = \Delta^x$. Hence $(k+1)^{\langle y^{m-1} \rangle} \cup (\zeta^x)^{\langle y^{m-1} \rangle} = \Omega_2 \subseteq \Delta^x$, and so $|\Delta^x| \geq k > |\Theta_1|$. Therefore Δ contains a point $\eta \notin \Theta_1$, and since $\Delta^y = \Delta$ it follows that $\eta^{\langle y \rangle} \subseteq \Delta$. If $\eta \in \Theta_3 \cup \Theta_4$, then Θ_3 or

$\Theta_4 \subseteq \Delta$. Hence either $\epsilon^x \in \Delta$ or $\zeta^x \in \Delta$ by Condition (iii)(c), and so $\Delta = \Delta^H = \Omega$, a contradiction. Therefore assume that $\Delta \subseteq \Theta_1 \cup \Theta_2 = \Omega_1$, and hence $\eta \in \Theta_2$, and so $\Delta = \Omega_1$ and H-block size is k. Now from $\Omega_2 \subseteq \Delta^x$, it follows that $\Delta^x = \Omega_2$. We reach a contradiction since $x \in X_1$, and so $\Omega_1^x \neq \Omega_2$.

Hence H is primitive and contains the p_k-cycle $y^{(k-p_k)(m-1)p_k'(k-p_k')} \in \mathcal{J}_c$. Thus $H = G$ by Theorem 4.3.4. □

Lemma 6.5.11. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *If $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. Let p_k, p_k' and p_m be as in Lemma 4.4.15. If either p_k or p_k' do not divide $m-1$ then, by interchanging p_k and p_k' if necessary, the result holds by Lemma 6.5.10. Since $x \notin \mathcal{J}$, Lemma 6.4.4 implies that there exist either $\alpha, \alpha^x \in \Omega_1$ or $\beta \in \Omega_1 \backslash \{1\}$ such that $\beta^x \notin \Omega_1 \cup \Omega_2$; there exist distinct points $\gamma, \gamma^x, \delta, \delta^x \in \mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega(\beta^x))$ and an element with cycle type $1^{n-kp_m} \cdot p_m^k$ is in $\mathcal{J}_w$.

By Lemma 4.2.1 an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_mp_k \cdot p_m(k-p_k-1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega(\gamma),\Omega(\gamma^x),\Omega(\delta),\Omega(\delta^x),\Omega(\beta^x)\in\mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_4^{\mathcal{M}})=m-p_m \\ \Omega_2\in\mathrm{Supp}(c_4^{\mathcal{M}})}}$$

with $1, \gamma, \delta^x \in \Theta_1$, $\delta \in \Theta_2$, $\gamma^x \in \Theta_3$, $k+1 \in \Theta_4$ and either α, α^x or $\beta, \beta^x \in \Theta_1$.

Hence, $H = \langle x, y\rangle$ is transitive. We claim that Lemma 4.2.15 implies that H is primitive. Let $(q_1, q_2, i, j, \upsilon, \phi) = (p_m, p_k, 4, 3, 1, \gamma)$, and either let $\psi = \alpha = \omega$ or $\psi = \beta = \omega$. From $p_k, p_k' \mid (m-1)$ it follows that $m > p_kp_k' > \frac{k^2}{4}$, and so $p_m > \frac{m}{2} > \frac{k^2}{8}$. Thus $p_m > k$ and $p_m \nmid k$. Hence $p_m \nmid |\Theta_4|$, $p_k \nmid |\Theta_3|$, and $p_mp_k \nmid |\Theta_l|$ for $2 \leq l \leq 4$. Also $1, \gamma \in \Theta_1$, $1^x = k+1 \in \Theta_4$ and $\gamma^x \in \Theta_3$. Finally $\psi, \psi^x, \omega, \omega^x \in \Theta_1$, $\psi \in \Omega_1 \cap \Theta_1 = 1^{\langle y^{pm}\rangle}$, and since $\omega \in \Omega_1$ and $\gamma \notin \Omega_1$, there exists $y \in \mathcal{Y}$ such that $\omega \in \gamma^{\langle y^{p_k}\rangle}$. Thus H satisfies Conditions (i), (ii) and (iii)(a) of Lemma 4.2.15, and so H is primitive.

Hence H is primitive and contains $y^{(m-p_m)k(k-p_k-1)p_k} \in \mathcal{J}_w$, an element of cycle type $1^{n-kp_m} \cdot p_m^k$. Therefore $H = G$ by Theorem 4.3.4. □

$|\Omega_1 \cap \mathrm{Supp}(x)| = 1$

We first assume that there exists $3 \leq j \leq m$ such that $|\Omega_j \cap \mathrm{Supp}(x)| \geq 4$, then we prove the general case, and finally prove Proposition 6.5.1.

Lemma 6.5.12. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *Assume that $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$, $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ and there exists $3 \leq j \leq m$ with*

$|\Omega_j \cap \operatorname{Supp}(x)| \geq 4$. *Then there exists* $y \in M$ *such that* $\langle x, y \rangle = G$.

Proof. Since $x \in X_1$ it follows that $|\Omega_2 \cap \operatorname{Supp}(x)| = 1$. By Proposition 6.2.6(iv) we may assume that there exists $\alpha \in \Omega_3$ and $i \in \{1, 4\}$ such that $\alpha^x \in \Omega_i$, and we may assume that $j = 3$, 4, or 5. Since $|\Omega_j \cap \operatorname{Supp}(x)| \geq 4$ and $|\Omega_j \cap \{\alpha, \alpha^x\}| \leq 1$ it follows that there exist $\beta \in (\Omega_j \cap \operatorname{Supp}(x)) \backslash \{\alpha, \alpha^x\}$ and $\gamma \in (\Omega_j \cap \operatorname{Supp}(x)) \backslash \{\alpha, \alpha^x, \beta, \beta^x\}$. If $p_k \nmid (m-2)$ then let $a := 2$; and otherwise let $a := 3$. Hence $p_k \nmid (m-a)$ and $a < m - a$.

By Lemma 4.2.1 an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1 c_2 c_3 c_4 \in M$ with

$$\mathcal{C}(y) = \underbrace{ap_k \cdot a \cdot \lambda(k - p_k - 1)}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=a \\ \Omega_1, \Omega_j \in \operatorname{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-a)k}_{\substack{l(c_4^{\mathcal{M}})=m-a \\ \{\Omega_2,\Omega_3,\Omega_4,\Omega_5\}\backslash\{\Omega_j\} \subseteq \operatorname{Supp}(c_4^{\mathcal{M}})}}$$

such that $\Omega_1^y = \Omega_j$, $1 \in \Theta_1$, $\beta \in \Theta_2$, $\gamma \in \Theta_3$, $k+1 \in \Theta_4$, $\beta^x \notin \Theta_2$, $\gamma^x \notin \Theta_2 \cup \Theta_3$.

Hence $H = H(y) = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is an imprimitive group preserving a non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since Θ_1 contains a point of $\Omega_1 \backslash \{1\} \subseteq \operatorname{Fix}(x)$ and $p_k \nmid |\Theta_i|$ for $i \neq 1$, it follows by Lemma 4.2.14(i) and (ii) that $l(c_1^{\mathcal{H}}) \neq 1, ap_k$.

First assume that $l(c_1^{\mathcal{H}}) = p_k$. Then we claim that $c_1^{\mathcal{H}} = c_4^{\mathcal{H}}$, a contradiction since $p_k \nmid |\Theta_4|$. By Lemma 4.2.13(iv) $|\Delta \cap \Omega_j \cap \Theta_1| = 1$. If $\Omega_j \cap \operatorname{Fix}(x) \neq \emptyset$ then there exists $y \in \mathcal{Y}$ such that $\Delta \cap \Omega_j \cap \operatorname{Fix}(x) \cap \Theta_1 \neq \emptyset$. Hence $\Delta^x = \Delta$ and so $k+1 \in \Delta$ and the claim holds by Lemma 4.2.11(i). Therefore we may assume that $\Omega_j \subseteq \operatorname{Supp}(x)$. Since $k > 10$ there exists $\epsilon \in \Omega_j \backslash \{1^{x^{-1}}, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}\}$ and so $\epsilon, \epsilon^x \notin \{1, k+1, \alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x\}$. Thus $\epsilon^x \in \operatorname{Supp}(x) \backslash \{1\}$ and so $\epsilon^x \notin \Omega_1$. If $\epsilon^x \in \Omega_j$, then by Lemma 4.2.13(iv) there exists $y \in \mathcal{Y}$ such that $\epsilon, \epsilon^x \in \Theta_1$ and $1, \epsilon \in \Delta$. Therefore $k+1, \epsilon^x \in \Delta^x$, and since $k+1 \in \Theta_4$ and $\epsilon^x \in \Theta_1$ the claim follows by Lemma 4.2.11(i). If $\epsilon^x \notin \Omega_j$, then there exists $y \in \mathcal{Y}$ and $\Gamma \in \mathcal{H}$ such that $\epsilon^x \in \Theta_4$ and Γ contains $\epsilon \in \Theta_1$ and a point of $\Omega_1 \backslash \{1\} \subseteq \operatorname{Fix}(x)$. Therefore $\Gamma^x = \Gamma$ and so $\epsilon^x \in \Gamma$. Thus the claim holds by Lemma 4.2.11(i), and so we reach a contradiction.

Now assume that $l(c_1^{\mathcal{H}}) = a$. Then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i), and so $\Delta^x = \Delta$ since $|\Omega_1 \cap \Theta_1 \cap \operatorname{Fix}(x)| \geq p_k - 1$. Therefore $k+1 \in \Delta$ and so $c_1^{\mathcal{H}} = c_4^{\mathcal{H}}$. Recall that $\alpha \in \Omega_3$ and $\alpha^x \in \Omega_i$ with $i = 1$ or 4. We claim there exists $y \in \mathcal{Y}$ such that $|\Delta \cap \{\alpha, \alpha^x\}| = 1$, contradicting the deduction that $\Delta^x = \Delta$. We now prove the claim by considering the possibilities for i and j. If $i = 1$, then from $\Omega_1 \cap \operatorname{Supp}(x) = 1$, it follows that $\alpha^x = 1 \in \Delta$. If $j = 3$, then there exists $y \in \mathcal{Y}$ with $\alpha \in \Theta_1$, and so $\alpha \in \Delta^y \cap \Theta_1 = \Omega_3 \cap \Theta_1$. If $j \neq 3$, then $\Omega_3 \subseteq \operatorname{Supp}(c_4^{\mathcal{M}})$ and there exists $y \in \mathcal{Y}$ such that

$(k+1)^y = \alpha$, and so $\alpha \in \Delta^y$. Therefore if $i = 1$, then the claim holds. Hence assume that $i = 4$. If $j = 4$, then $\Omega_4 \in \mathrm{Supp}(c_1^{\mathcal{M}})$ and $\Omega_3 \in \mathrm{Supp}(c_4^{\mathcal{M}})$, and so there exists $y \in \mathcal{Y}$ such that $\alpha^x \in \Omega_4 \cap \Theta_1 = \Delta^y \cap \Theta_1$ and $\alpha = (k+1)^{y^a} \in \Delta$. If $j = 3$, then $\Omega_3 \in \mathrm{Supp}(c_1^{\mathcal{M}})$ and $\Omega_4 \in \mathrm{Supp}(c_4^{\mathcal{M}})$. Hence $\alpha \in \Omega_3 \cap \Theta_1 = \Delta^y \cap \Theta_1$ and there exists $y \in \mathcal{Y}$ such that $\alpha^x = (k+1)^{y^a} \in \Delta$. If $j = 5$, then $\Omega_3, \Omega_4 \in \mathrm{Supp}(c_4^{\mathcal{M}})$ and there exists $y \in \mathcal{Y}$ such that $\alpha^x = \alpha^y$. Hence the claim holds in all cases and we reach the desired contradiction.

Therefore H is primitive and contains $y^{a(k-p_k-1)(m-a)k}$, an element of cycle type $1^{n-ap_k} \cdot {p_k}^a$. Now $a \in \{2,3\}$, $p_k \geq 5$ and $n - ap_k > (m-3)p_k > 3$, and so $y^{a(k-p_k-1)(m-a)k} \in \mathcal{J}_w$. Hence $H = G$ by Theorem 4.3.4. □

Lemma 6.5.13. *Let $m \geq 19$, let $k \geq 28$, and let G and M be as in Hypothesis 6.2.7*(B). *If $x \in X_1 \backslash (\hat{M} \cup \mathcal{J})$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If there exists $3 \leq j \leq m$ such that $|\mathrm{Supp}(x) \cap \Omega_j| \geq 4$, then the result holds by Lemma 6.5.12. Hence we may assume that otherwise.

Therefore $|\Omega_1 \cap \mathrm{Supp}(x)| = |\Omega_2 \cap \mathrm{Supp}(x)| = 1$ and $|\Omega_j \cap \mathrm{Supp}(x)| \leq 3$ for $j \neq 1, 2$. Since $x \notin \mathcal{J}_s$ it follows that $|\mathrm{Supp}(x)| \geq 15 > 1 + 1 + 4(3)$, and so there exist at least seven M-blocks containing points of $\mathrm{Supp}(x)$. By Proposition 6.2.6(iv) we may assume that $\alpha \in \Omega_3$ such that $\alpha^x \in \Omega_1 \cup \Omega_4$, $\Omega_1, \ldots, \Omega_7$ contain points of $\mathrm{Supp}(x)$, and there exist $\beta \in \Omega_5 \cap \mathrm{Supp}(x)$ and $\gamma \in \Omega_6 \cap \mathrm{Supp}(x)$ such that $\beta^x \neq \gamma$.

Let p_k and $p_k{}'$ be as in Lemma 4.4.12. If $p_k \nmid (m-2)$ then let $a := 2$ and otherwise let $a := 3$, so that $p_k \nmid (m-a)$. By Lemma 4.2.1, an element composed of four cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $y = c_1c_2c_3c_4 \in M$ with

$$\mathcal{C}(y) = \underbrace{ap_k \cdot a(k-p_k)}_{l(c_1c_2)=a} \cdot \underbrace{(m-a)p_k{}' \cdot (m-a)(k-p_k{}')}_{l((c_3c_4)^{\mathcal{M}})=m-a}$$

satisfying the following.

(i) If $a = 2$ then $(c_1c_2)^{\mathcal{M}} = (\Omega_1, \Omega_5)$, and if $a = 3$ then $(c_1c_2)^{\mathcal{M}} = (\Omega_1, \Omega_5, \Omega_8)$.

(ii) $1 \in \Theta_1$, $\beta \in \Theta_2$, $k+1 \in \Theta_3$, $\gamma \in \Theta_4$, $\beta^x \in \Theta_1 \cup \Theta_3$ and $\gamma^x \notin \Theta_4$.

(iii) For all $\Omega_i \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})$ there exists $\delta_i \in \Omega_i \cap \mathrm{Fix}(x) \cap \Theta_1$.

Condition (iii) is automatically satisfied since $|\Omega_i \cap \mathrm{Supp}(x)| \leq 3 < p_k$ for $1 \leq i \leq m$. By Condition (ii), $H = H(y) = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive and let $\mathcal{H}$ be a non-trivial block system for H. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$, Lemma 4.2.14(i) implies that $l(c_1^{\mathcal{H}}) \neq 1$. Since $p_k \nmid |\Theta_i|$ for $i \neq 1$, Lemma 4.2.14(ii) implies that $l(c_1^{\mathcal{H}}) \neq ap_k$.

Assume that $l(c_1^{\mathcal{H}}) = p_k$. Then $|\Delta \cap \Omega_j \cap \Theta_1| = 1$ for $\Omega_j \in \mathrm{Supp}(c_1^{\mathcal{M}})$ by Lemma 4.2.13(iv). Hence there exists $y \in \mathcal{Y}$ such that $1, \delta_5 \in \Delta$, and so $\Delta^x = \Delta$ and $k+1 \in \Delta$. Since $k+1 \in \Theta_3$ and $p_k \nmid |\Theta_3|$ we reach a contradiction by Lemma 4.2.14(iii).

Suppose that $l(c_1^{\mathcal{H}}) = a = 3$ (the case for $a = 2$ is almost identical). Then there exists $\Delta_1 := \Delta, \Delta_2, \Delta_3 \in \mathcal{H}$ such that $c_1^{\mathcal{H}} = (\Delta_1, \Delta_2, \Delta_3)$. By Lemma 4.2.13(i) $\Delta_1 \cap \Theta_1 = \Omega_1 \cap \Theta_1$, $\Delta_2 \cap \Theta_1 = \Omega_5 \cap \Theta_1$ and $\Delta_3 \cap \Theta_1 = \Omega_8 \cap \Theta_1$. Hence by Condition (iii), Δ_1, Δ_2 and Δ_3 are all fixed by x. Then $k+1 \in \Delta_1$ and by the transitivity of H and Lemma 4.2.11(i), it follows that $y^{\mathcal{H}} = (\Delta_1, \Delta_2, \Delta_3)$. Recall that $\alpha \in \Omega_3$ and $\alpha^x \in \Omega_i$ for $i = 1$ or 4. If $i = 1$, then $\alpha^x = 1$ and so $\alpha^x \in \Delta_1$. There exists $y \in \mathcal{Y}$ with $(k+1)^y = \alpha$, so that $\alpha \in \Delta_2$. If $i = 4$, then there exists $y \in \mathcal{Y}$ with $(k+1)^y = \alpha$ and $(k+1)^{y^2} = \alpha^x$, so that $\alpha \in \Delta_2$ and $\alpha^x \in \Delta_3$. In either case we reach a contradiction since each block was fixed by x.

Therefore H is a primitive group containing $y^{a(k-p_k)(m-a)p_k'(k-p_k')}$, an element of cycle type $1^{n-ap_k} \cdot {p_k}^a$. As in the previous proof, $a \in \{2,3\}$, $p_k \geq 5$ and $n - ap_k > (m-3)p_k > 3$. Hence $y^{a(k-p_k)(m-a)p_k'(k-p_k')} \in \mathcal{J}_w$ and so $H = G$ by Theorem 4.3.4. □

Proof of Proposition 6.5.1. First suppose that $x \in \hat{M}$. If $|\Omega_1 \cap \mathrm{Supp}(x)| > 3$, then the result holds by Lemma 6.5.2. If $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \not\subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for any $3 \leq i, j \leq m$, then the result holds by Lemma 6.5.5. If $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$ and $\mathrm{Supp}(x) \subseteq \Omega_1 \cup \Omega_2 \cup \Omega_i \cup \Omega_j$ for some i, j, then the result holds by Lemma 6.5.9.

Now suppose that $x \notin \hat{M}$. If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, then the result holds by Lemma 6.5.11. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then the result holds by Lemma 6.5.13. □

6.6 Small m or small k

Recall that $m, k \geq 2$, $n = mk$, $G = \mathrm{S}_n$ or A_n, and $M = (\mathrm{S}_k \,\mathrm{wr}\, \mathrm{S}_m) \cap G$. Here we consider m and k in Regions one, two or six of Figure 6.1. In particular we consider $2 \leq k \leq 6$ and $m \geq 23$; then $7 \leq k \leq 28$ for $m \geq 4k - 1$; and finally $2 \leq m \leq 18$ and $k \geq \max\{4m - 1, 28\}$.

In this section we let $x \in X_1$, and so $1^x = k+1$, $\Omega_1^x \notin \mathcal{M}$ and $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_2 \cap \mathrm{Supp}(x)|$.

6.6.1 Region one - $2 \leq k \leq 6$ and $m \geq 23$

For $2 \leq k \leq 6$ there is no Bertrand prime p_k with $\frac{k}{2} < p_k < k - 1$. As a result we require some more technical lemmas on the existence of certain points, and so this subsection is the largest of the section. We consider Hypothesis 6.2.7(A) and (B) separately.

Hypothesis 6.2.7(A)

We begin with two preliminary lemmas.

Lemma 6.6.1. *Let $2 \leq k \leq 6$ and let $m \geq 23$. If $x \in X_1 \backslash \mathcal{J}$ and $|\mathrm{Supp}(x)| > \max\{7, 2k+1\}$, then there exists $\alpha \in \mathrm{Supp}(x)\backslash(\{k+1\} \cup \Omega_2^x \cup \Omega_1)$ such that the following hold.*

(i) *If $k = 2$, then $\Omega_1^x \nsubseteq \{k+1\} \cup \Omega(\alpha)$.*

(ii) *If $k > 2$ and $\Omega_1^x \subseteq \{k+1\} \cup \Omega(\alpha)$, then $\alpha^{x^{-1}} \notin \Omega(\alpha)$.*

Proof. Since $|\mathrm{Supp}(x)| > 2k+1$ there exists $\alpha \in \mathrm{Supp}(x)\backslash(\{k+1\} \cup \Omega_2^x \cup \Omega_1)$. We show that there exists $\beta \in \mathrm{Supp}(x)$ such that, by exchanging α and β if necessary, the lemma holds.

(i) If $k = 2$, then $\max\{7, 2k+1\} = 7$ and $|\mathrm{Supp}(x)| > 7 \geq |\{k+1\} \cup \Omega(\alpha) \cup \Omega_2^x \cup \Omega_1|$. Hence there exists $\beta \in \mathrm{Supp}(x)\backslash(\{k+1\} \cup \Omega(\alpha) \cup \Omega_2^x \cup \Omega_1)$ and so $\Omega(\alpha) \neq \Omega(\beta)$. By interchanging α and β if necessary $\Omega_1^x \nsubseteq \{k+1\} \cup \Omega(\alpha)$.

(ii) Now assume that $k > 2$ and $\Omega_1^x \subseteq \{k+1\} \cup \Omega(\alpha)$. From $x \in X_1$, it follows that $\Omega_1^x \notin \mathcal{M}$, and so in particular $\Omega_1^x \neq \Omega(\alpha)$. Thus $\Omega_1^x \subseteq \{k+1\} \cup \Omega(\alpha)$ implies that $k+1 \in \Omega_1^x \backslash \Omega(\alpha)$. Hence there exists $\gamma \in \Omega(\alpha)\backslash\Omega_1^x$ such that

$$\Omega(\alpha) = (\Omega_1\backslash\{1\})^x \,\dot\cup\, \{\gamma\}. \tag{6.11}$$

Hence

$$\Omega(\alpha) \cap \Omega_2^x = \left[(\Omega_1\backslash\{1\})^x \cap \Omega_2^x\right] \cup \left[\{\gamma\} \cap \Omega_2^x\right] = \emptyset \cup \left[\{\gamma\} \cap \Omega_2^x\right] \subseteq \{\gamma\}. \tag{6.12}$$

In addition, (6.11) implies that $|\Omega_1^x \cap \Omega(\alpha)| = k - 1 > 1$. Thus there exists $\beta \in \Omega_1^x \cap \Omega(\alpha)$, and it follows by (6.11) and (6.12) that $\beta \notin \{k+1\} \cup \Omega_2^x \cup \Omega_1$. Furthermore since $\alpha \notin \Omega_1$ it follows by (6.11) that $\Omega_1^x \cap \Omega_1 = \emptyset$. Thus Ω_1, and so Ω_1^x also, are contained in $\mathrm{Supp}(x)$. Hence

$$\beta \in \Omega_1^x \backslash(\{k+1\} \cup \Omega_2^x \cup \Omega_1) \subseteq \mathrm{Supp}(x)\backslash(\{k+1\} \cup \Omega_2^x \cup \Omega_1).$$

Finally, $\alpha, \beta \in \Omega(\alpha) \neq \Omega_1$. Thus $\beta^x \in \Omega_1^x$ gives $\beta^{x^{-1}} \in \Omega_1 \neq \Omega(\beta)$. Therefore the result follows with β in place of α.

□

Lemma 6.6.2. *Let $2 \leq k \leq 6$, let $m \geq 23$ and let α be as in Lemma 6.6.1. Then at least one of the following holds:*

(i) *$\Omega_1^x \cap \Omega_1 \neq \emptyset$;*

(ii) *there exists* $\beta \in \Omega_1$ *such that* $\beta^x \notin \Omega_2 \cup \Omega(\alpha)$*;*

(iii) *there exists* $\gamma \in \Omega_1 \backslash \{1\}$ *such that* $\gamma^x \in \Omega_2$*; or*

(iv) $\Omega_1^x \subseteq \{k+1\} \cup \Omega_2$ *and there exists* $\delta \in \Omega_1 \backslash \{1\}$ *such that* $\delta^x \in \Omega(\alpha) \backslash \{\alpha\}$*.*

Proof. Assume that (i)-(iii) do not hold. Then (ii) not holding implies that $\Omega_1^x \subseteq \Omega_2 \cup \Omega(\alpha)$, and that (iii) not holding implies that $(\Omega_1 \backslash \{1\})^x \cap \Omega_2 = \emptyset$. Hence $\Omega_1^x \subseteq \{k+1\} \cup \Omega(\alpha)$. If $k = 2$, then we reach a contradiction by Lemma 6.6.1(i). Hence let $k > 2$ and $\delta \in \Omega_1 \backslash \{1, \alpha^{x^{-1}}\}$, so that $\delta^x \in \Omega(\alpha) \backslash \{\alpha\}$. □

Lemma 6.6.3. *Let* $2 \leq k \leq 6$*, let* $m \geq 23$*, and let* G *and* M *be as in Hypothesis 6.2.7*(A)*. If* $x \in X_1 \backslash \mathcal{J}$*, then there exists* $y \in M$ *such that* $\langle x, y \rangle = G$*.*

Proof. We first show that if $|\mathrm{Supp}(x)| \leq \max\{7, 2k+1\}$, then $|\mathrm{Supp}(x)| \leq 2(\sqrt{n} - 1)$, and so $x \in \mathcal{J}$. If $k = 2$, then $\max\{7, 2k+1\} = 7$ and

$$|\mathrm{Supp}(x)| \leq 7 < 2(\sqrt{2 \cdot 11} - 1) \leq 2(\sqrt{mk} - 1).$$

If $k \geq 3$, then $\max\{7, 2k+1\} = 2k+1$, we show this is less that $2(\sqrt{mk} - 1)$. Let $f(k) = 4k^2 - 44k + 9$. Then f has roots in $0 < k < 1$ and $10 < k < 11$. Hence $f(k) < 0$ for $3 \leq k \leq 6$, and so

$$(2k+3)^2 = 4k^2 + 12k + 9 < 56k = 4(14k),$$

Therefore $2k + 1 < 2(\sqrt{14k} - 1) \leq 2(\sqrt{mk} - 1)$. Thus if $|\mathrm{Supp}(x)| \leq \max\{7, 2k+1\}$, then $x \in \mathcal{J}_s$.

Therefore assume that $|\mathrm{Supp}(x)| > \max\{7, 2k+1\}$. Let α be as in Lemma 6.6.1, let β, γ or δ be as in Lemma 6.6.2. By Lemma 4.4.17 there exists a prime p_m such that $p_m \leq m - 3$. Note that $p_m > \frac{m}{2} \geq 7$ and so $p_m \nmid k(k-1)$.

Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_m \cdot p_m(k-1)}_{\substack{l((c_1c_2)^{\mathcal{M}})=p_m \\ \Omega_2,\Omega(\alpha)\in\mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_3^{\mathcal{M}})=m-p_m \\ \Omega_1\in\mathrm{Supp}(c_3^{\mathcal{M}})}}$$

such that the following hold.

(i) $k+1 \in \Theta_1$, $\alpha \in \Theta_2$ and $1 \in \Theta_3$.

(ii) If $\alpha^{x^{-1}} \notin \Omega(\alpha)$, then $\alpha^{x^{-1}} \in \Theta_3$; and otherwise $\alpha^{x^{-1}} \in \Theta_1$

(iii) If β exists, then $\beta, \beta^x \in \Theta_3$. If γ exists, then $\gamma \in \Theta_3$ and $\gamma^x \in \Theta_2$. If δ exists, then $\delta \in \Theta_3$; while $\delta^x \in \Theta_2$ if $\Omega(\alpha) = \Omega_2$, and $\delta^x \in \Theta_1$ otherwise.

We begin by justifying why $\mathcal{Y} \neq \emptyset$.

By Lemma 6.6.1 $\alpha \notin \Omega_2^x$, and so $\alpha^{x^{-1}} \notin \Omega_2$. Hence if $\alpha^{x^{-1}} \notin \Omega(\alpha)$, then $\Omega(\alpha^{x^{-1}}) \neq \Omega_1, \Omega(\alpha)$ and so we can insist that $\Omega(\alpha^{x^{-1}}) \in \mathrm{Supp}(c_3^{\mathcal{M}})$, and so $\alpha^{x^{-1}} \in \Theta_3$. If $\alpha^{x^{-1}} \in \Omega(\alpha)$, then $\alpha^{x^{-1}} \in \Theta_1 \cup \Theta_2$ and so since $\alpha^{x^{-1}} \notin \Omega_2$ it follows we can place $\alpha^{x^{-1}}$ in Θ_1. If β exists as in Lemma 6.6.2, then $\beta^x \notin \Omega_2 \cup \Omega(\alpha^x)$ and so $\Omega(\beta^x), \Omega_2, \Omega(\alpha^x)$ are distinct. So far $\mathrm{Supp}(c_3^{\mathcal{M}})$ contains Ω_1 and possibly $\Omega(\alpha^{x^{-1}})$, and by Lemma 4.4.17 $m - p_m \geq 3$. Hence we can insist that $\Omega(\beta^x) \in \mathrm{Supp}(c_3^{\mathcal{M}})$ so that $\beta^x \in \Theta_3$.

If $\gamma \in \Omega_1 \backslash \{1\}$ exists as in Lemma 6.6.2, then $\gamma^x \in \Omega_2 \subseteq \Theta_1 \cup \Theta_2$. From $\gamma \neq 1$ it follows that $\gamma^x \neq k+1$, and so $\gamma^x \in \Theta_2$ automatically.

Finally, if $\delta \in \Omega_1 \backslash \{1\}$ exists as in Lemma 6.6.2, then $\delta^x \in \Omega(\alpha) \backslash \{\alpha\} \subseteq \Theta_1 \cup \Theta_2$. Since $\delta \neq 1$ it follows that $\delta \neq k+1, \alpha$. Hence if $\Omega_2 = \Omega(\alpha)$, then we can insist that $\delta^x \in \Theta_2$, and if $\Omega_2 \neq \Omega(\alpha)$ that $\delta^x \in \Theta_1$.

It is clear by Conditions (i) and (ii) that $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $k+1 \in \Delta$.

If $l(c_1^{\mathcal{H}}) = 1$, then $\Delta^y = \Delta$ and $\Theta_1 \subseteq \Delta$. Since $|\Theta_1| = p_m$ and $p_m \nmid n$ it follows by Lemma 4.2.6 that there exists $\epsilon \in \Delta \backslash \Theta_1$. Hence $\epsilon^Y \cup \Theta_1 \subseteq \Delta$. If $\epsilon \in \Theta_2$, then $|\Delta| > \frac{n}{2}$, a contradiction. If $\epsilon \in \Theta_3$, then $1, k+1 \in \Delta$ and so $\Delta^H = \Delta$, a contradiction.

Assume that $l(c_1^{\mathcal{H}}) = p_m$. Since $p_m \nmid |\Theta_3|$, Lemma 4.2.11(iv) implies that $\Delta \cap \Theta_3 = \emptyset$. Since H is non-trivial, it follows by Lemma 4.2.11(i) that $c_2^{\mathcal{H}} = c_1^{\mathcal{H}}$. Hence block size is k, and so $l(c_3^{\mathcal{H}}) = m - p_m$. Therefore by Lemma 4.2.13(i) $c_3^{\mathcal{H}} = c_3^{\mathcal{M}}$. Thus there exists $\Gamma \in \mathcal{H}$ with $\Gamma = \Omega_1$. Since $1^x = k+1$ it follows that $\Gamma^x = \Delta$. If $\Omega_1^x \cap \Omega_1 \neq \emptyset$, then $\Gamma = \Delta$, a contradiction since $\Delta \cap \Theta_3 = \emptyset$. If β exists, then $\beta \in \Gamma$ and so $\beta^x \in \Delta \cap \Theta_3$ by Condition (iii), a contradiction. If γ exists, then $1, \gamma \in \Gamma$ and so $k+1, \gamma^x \in \Delta$. Since $(k+1)^{y^{pm}} = k+1$, Condition (iii) implies that $\Delta = \{k+1\} \cup (\gamma^x)^{\langle y^{pm} \rangle} = \Omega_2$, a contradiction since $\Gamma = \Omega_1$ and $\Omega_1^x \neq \Omega_2$.

Hence if Lemma 6.6.2(i)-(iii) hold, then $\Omega_1^x \subseteq \{k+1\} \cup \Omega(\alpha)$ and δ exists. Hence $\delta \in \Omega_1 = \Gamma$ and by Lemma 6.6.1 $k > 2$ and $\alpha^{x^{-1}} \notin \Omega(\alpha)$. Therefore $k+1, \delta^x \in \Delta$. If $\Omega(\alpha) = \Omega_2$, then $\Delta = \{k+1\} \cup (\delta^x)^{\langle y^{pm} \rangle} = \Omega_2$, a contradiction since $\Omega_1^x \neq \Omega_2$. If $\Omega(\alpha) \neq \Omega_2$, then $|\Delta \cap \Theta_1| = 2$, a contradiction.

Hence H is a primitive group containing $y_1 = y^{(k-1)(m-p_m)k}$ which has cycle type $1^{n-p_mk} \cdot p_m^k$. Note that since $2 \leq k \leq 6$ and $11 \leq p_m \leq m-3$, it follows that

$$n = mk \geq k(p_m + 3) \geq kp_m + 3k \geq kp_m + 6.$$

Hence $y_1 \in \mathcal{J}_w$ and so $H = G$ by Theorem 4.3.4. □

Hypothesis 6.2.7(B)

We begin with a preliminary lemma.

Lemma 6.6.4. *Let $2 \leq k \leq 6$, let $m \geq 23$ and let $x \in X_1 \backslash \mathcal{J}$. If $|\mathrm{Supp}(x)| > 3k+3$, then the following holds.*

(i) *If $k > 2$, then there exist distinct points $\alpha, \alpha^x, \beta, \beta^x \in \mathrm{Supp}(x) \backslash \Omega_2$ such that $\alpha, \beta \neq 1$ and $\Omega(\alpha) \neq \Omega(\beta)$.*

(ii) *If $k = 2$ and $x \notin \hat{M}$, then there exist distinct points $\gamma, \gamma^x, \delta \in \mathrm{Supp}(x)$ such that $\gamma \in \Omega_3$, $\gamma^x \notin \Omega_3$, $\delta \notin \Omega_1 \cup \Omega_2$ and $\delta^x \notin \Omega_2$.*

Proof. (i) Since $|\mathrm{Supp}(x)| > 3k+3$ there exists $\alpha \in \mathrm{Supp}(x) \backslash (\Omega_2 \cup \Omega_2^{x^{-1}})$ and $\beta \in \mathrm{Supp}(x) \backslash (\Omega_2 \cup \Omega_2^{x^{-1}} \cup \Omega(\alpha) \cup \{\alpha^x, \alpha^{x^{-1}}\})$. Hence $\alpha, \alpha^x, \beta, \beta^x \notin \Omega_2$ and $\Omega(\alpha) \neq \Omega(\beta)$. Since $1^x \in \Omega_2$ and $\alpha^x, \beta^x \notin \Omega_2$ it follows that $\alpha, \beta \neq 1$.

(ii) Since $x \in X_1 \backslash \hat{M}$, Proposition 6.2.6(i) implies that we may assume that there exists $\gamma \in \Omega_3$ such that $\gamma^x \notin \Omega_3$. Since $1 = (k+1)^{x^{-1}} \in \Omega_1 \cap \Omega_2^{x^{-1}}$, it follows by inclusion-exclusion that $|\Omega_1 \cup \Omega_2^{x^{-1}}| \leq 3$. Therefore

$$|\Omega_2 \cup \Omega_2^{x^{-1}} \cup \Omega_1 \cup \Omega(\gamma) \cup \Omega(\gamma^x)| \leq 2+3+2+2 = 9 \leq 3k+3.$$

Hence there exists $\delta \in \mathrm{Supp}(x) \backslash (\Omega_2 \cup \Omega_2^{x^{-1}} \cup \Omega_1 \cup \Omega(\gamma) \cup \Omega(\gamma^x))$. □

Lemma 6.6.5. *Let $2 \leq k \leq 6$, let $m \geq 23$ and let G and M be as in Hypothesis 6.2.7*(B). *If $x \in X_1 \backslash \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. Since $2 \leq k \leq 6$, it follows that

$$9k + 24 + \frac{16}{k} < 9(6) + 24 + \frac{16}{2} = 86 < 92 \leq 4m.$$

Hence $(3k+4)^2 = 9k^2 + 24k + 16 \leq 4mk$, and so $3k+2 \leq 2(\sqrt{mk}-1)$. Hence if $|\mathrm{Supp}(x)| \leq 3k+2$, then $x \in \mathcal{J}_s$. Therefore, we may assume otherwise and let α, β or γ, δ be as in Lemma 6.6.4. Since $m \geq 23$ it follows that $p_m \geq 13$, and so $(p_m, k) = 1$. Let $\mathcal{Y}$ be the set of elements $y = c_1 c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_m k}_{\substack{l(c_1^{\mathcal{M}}) = p_m \\ \Omega_1 \in \mathrm{Supp}(c_1^{\mathcal{M}})}} \cdot \underbrace{(m - p_m)k}_{\substack{l(c_2^{\mathcal{M}}) = m - p_m \\ \Omega_2 \in \mathrm{Supp}(c_2^{\mathcal{M}})}}$$

satisfying the following.

(i) If $k > 2$, then let $\alpha, \alpha^x, \beta, \beta^x \in \Theta_1$ and $\alpha^{y^k} = \beta$.

(a) If $\Omega(\alpha^x) = \Omega(\beta^x)$ let $(\alpha^x)^{y^{pm}} = \beta^x$.

(b) If $\Omega(\alpha^x) \neq \Omega(\beta^x)$ and either $\alpha^x \notin \Omega(\alpha) \cup \Omega(\beta)$ or $\beta^x \notin \Omega(\alpha) \cup \Omega(\beta)$, then let $(\alpha^x)^y = \beta^x$.

(c) If $\{\Omega(\alpha), \Omega(\beta)\} = \{\Omega(\alpha^x), \Omega(\beta^x)\}$, then let $\{\alpha^{y^{pm}}, \beta^{y^{2pm}}\} = \{\alpha^x, \beta^x\}$.

(ii) If $k = 2$, then let $\Omega_3 \in \mathrm{Supp}(c_1^{\mathcal{M}})$. In addition, if $x \notin \hat{M}$ do the following.

(a) If $\gamma^x \notin \Omega_1 \cup \Omega_2$, then let $\{1, \gamma, \gamma^x\} \subseteq \{1, 1^{y^2}, 1^{y^4}\}$ and $\delta^{y^i} = \delta^x$ with i odd.

(b) If $\gamma^x \in \Omega_1 \backslash \{1\}$, then let $1^y = \gamma$ and $\delta^{y^i} = \delta^x$ with i odd.

(c) If $\gamma^x = 1$, then let $1^{y^2} = \gamma$ and $\delta^{y^i} = \delta^x$ with i odd.

(d) If $\gamma^x \in \Omega_2$, then let $1^y = \gamma$ if $2 \mid (m - p_m)$, and let $\gamma = 1^{y^2}$ if $2 \nmid (m - p_m)$.

(iii) If 2 is a proper divisor of k let $\epsilon := 1^{y^{2p_m}}$, and if 3 is a proper divisor of k let $\zeta := 1^{y^{3p_m}}$. If $\epsilon^x \notin \Omega_2$, then let $\Omega(\epsilon^x) \in \mathrm{Supp}(c_1^{\mathcal{M}})$, otherwise let $\epsilon^x = (k+1)^{y^{(m-p_m)}}$. If $\zeta^x \notin \Omega_2$, then let $\Omega(\zeta^x) \in \mathrm{Supp}(c_1^{\mathcal{M}})$, otherwise let $\zeta^x = (k+1)^{y^{-(m-p_m)}}$.

The placements of $\alpha^{y^k} = \beta$ in Condition (i) can hold since $(k, p_m) = 1$. If $\Omega(\delta) = \Omega(\delta^x)$, then the condition on δ^{y^i} in (ii) is automatic since p_m is odd. If $\Omega(\delta) \neq \Omega(\delta^x)$, then there are no other restrictions on $\Omega(\delta)$, and so we can place $\Omega(\delta)$ in $y^{\mathcal{M}}$ to satisfy Hence Condition (ii).

Since $1 \in \Theta_1$ and $k + 1 \in \Theta_2$ it follows that $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is an imprimitive group with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $|\Theta_1| > |\Theta_2|$ and $p_m \nmid (m - p_m)k$, Lemma 4.2.14(i) and (ii) imply that $l(c_1^{\mathcal{H}}) \neq 1, p_m k$. If $l(c_1^{\mathcal{H}}) = p_m$, then from $p_m \nmid |\Theta_2|$, Lemma 4.2.11(iv) implies that $\Delta \subseteq \Theta_1$ and block size is k. Hence $l(c_2^{\mathcal{H}}) = m - p_m$, and so $\mathcal{H}$ is the set of translates under y of $1^{\langle y^{p_m} \rangle}$ and $(k+1)^{\langle y^{(m-p_m)} \rangle}$. Since $\Omega_1 = 1^{\langle y^{p_m} \rangle}$ and $\Omega_2 = (k+1)^{\langle y^{(m-p_m)} \rangle}$, it follows that $\mathcal{H} = \mathcal{M}$, a contradiction since $x \notin M$.

First assume that $l(c_1^{\mathcal{H}}) = dp_m$ for $1 < d < k$ a divisor of k. Then $d = 2$ or 3. Let $l(c_1^{\mathcal{H}}) = 2p_m$, the argument for $d = 3$ is very similar. Since $p_m \nmid |\Theta_2|$ it follows by Lemma 4.2.11(iv) that $\Delta \subseteq \Theta_1$. Hence by Lemma 4.2.11(i), for all $\Gamma \in \mathcal{H}$, either $\Gamma \subseteq \Theta_1$ or $\Gamma \subseteq \Theta_2$. In addition block size is $\frac{k}{2}$. By Lemma 4.2.13(iii) $\Delta \subseteq \Omega_1$ and $\epsilon \in \Delta$. If $\epsilon^x \notin \Omega_2$, then Δ^x contains $\epsilon^x \in \Theta_1$ and $k + 1 \in \Theta_2$, a contradiction. If $\epsilon^x \in \Omega_2$, then Δ^x is left invariant by $y^{(m-p_m)}$. Hence $|\Delta^x| \geq |(k+1)^{\langle y^{(m-pm)} \rangle}| = k > \frac{k}{2}$, a contradiction.

Let $k > 2$, let $e > 1$ be a divisor of k, and assume that $l(c_1^{\mathcal{H}}) = e$. Let $\Gamma \in \mathcal{H}$ with $\alpha \in \Gamma$. Then $\alpha^{\langle y^k \rangle} \subseteq \alpha^{\langle y^e \rangle} \subseteq \Gamma$ and so Γ contains α and $\alpha^{y^k} = \beta$. If

$\{\Omega(\alpha), \Omega(\beta)\} = \{\Omega(\alpha^x), \Omega(\beta^x)\}$ or $\Omega(\alpha^x) = \Omega(\beta^x)$, then by Condition (i)(a) and (i)(c) Γ^x is fixed by y^{p_m}. Hence $p_m \mid l(c_1^{\mathcal{H}})$, a contradiction. Therefore, either $\alpha^x \notin \Omega(\alpha) \cup \Omega(\beta)$ or $\beta^x \notin \Omega(\alpha) \cup \Omega(\beta)$. Hence by Condition (i)(b) $\alpha^{xy} = \beta^x$, and so Γ^x is fixed by y. Therefore $c_1^{\mathcal{H}} = (\Gamma^x)$, a contradiction since $l(c_1^{\mathcal{H}}) = e > 1$.

It remains to consider the case of that $k = 2$ and $c_1^{\mathcal{H}} = (\Delta, \Gamma)$ for some $\Gamma \in \mathcal{H}$. First let $x \in \hat{M}$. Lemma 6.6.4 and Conditions (i)-(iii) imply only that $\Omega_1, \Omega_3 \in \mathrm{Supp}(c_1^{\mathcal{H}})$. For $1 \leq i \leq m$ let $\Omega_i = \{\eta_i, \iota_i\}$ so that $\eta_1 = 1$ and $\eta_2 = k+1$. Since $\Omega_1^x \neq \Omega_2$ it follows that $\iota_1 = 2, \iota_2 = k+1 \in \mathrm{Fix}(x)$. Hence

$$x = (1, k+1)(\eta_{i_1}, \iota_{i_1}) \cdots (\eta_{i_r}, \iota_{i_r})$$

with $i_1, \ldots, i_r \in \{3, \ldots, m\}$. Since $|\mathrm{Supp}(x)| > 3k+3$, it follows that $r \geq 4$, and so $(\eta_{i_1}, \iota_{i_1})$ is a cycle of x. By Lemma 4.2.13(iv) $|\Delta \cap \Omega_{i_1}| = 1 = |\Gamma \cap \Omega_{i_1}|$, and so $\Gamma^x = \Delta$. Again by Lemma 4.2.13(iv), $\Delta \cap \Omega_1 = \{1\}$ and so $s_1 = 2 \in \Gamma$. Hence $\Gamma^x = \Gamma$, a contradiction. Thus for the remainder of the proof we may assume that $x \notin \hat{M}$.

If $\gamma^x \notin \Omega_1 \cup \Omega_2$, then by Condition (ii)(a) $\gamma, \gamma^x \in \Delta$ and so $\Delta^x = \Delta$. However, again by Condition (ii)(a), Δ contains exactly one of δ, δ^x, and so we reach a contradiction. If $\gamma^x \in \Omega_1 \backslash \{1\}$, then by Condition (ii)(b) $\gamma \in \Gamma$ and by Lemma 4.2.13(iv) $\gamma^x \in \Gamma$. Hence $\gamma, \gamma^x \in \Gamma$, a contradiction since Γ contains exactly one of δ, δ^x by Condition (ii)(b). If $\gamma^x = 1$, then by Condition (ii)(c) it follows that $\gamma, \gamma^x \in \Delta$ and that Δ contains exactly one of δ, δ^x, a contradiction. Hence $\gamma^x \in \Omega_2$, and so $\Omega_2 = \{k+1, \gamma^x\}$. Since $|\Delta \cap \Theta_1| = p_m$ and $p_m \nmid n$ it follows by Lemma 4.2.6 that $y^{\mathcal{H}} = (\Delta, \Gamma)$. If $2 \mid (m - p_m)$, then by Lemma 4.2.13(ii) $\Delta \cap \Theta_2$ and $\Gamma \cap \Theta_2$ are a union of M-blocks. Hence $\{k+1, \gamma^x\} = \Omega_2 \subseteq \Delta^x$, a contradiction since $1 \in \Delta$ and $\gamma \in \Gamma$ by Condition (ii)(d). If $2 \nmid (m - p_m)$, then by Condition (ii)(b) $1, \gamma \in \Delta$. However by Lemma 4.2.13(iv) Δ contains exactly one of $\Omega_1 = \{k+1, \gamma^x\}$, a contradiction.

Hence H is a primitive group containing $y^{k(m-p_m)}$, with cycle type $1^{n-p_m k} \cdot p_m^k$. Now $2 \leq k \leq 6$ and $p_m > 11$ and $n - p_m k = (m - p_m)k \geq 2k$. Hence $y^{k(m-p_m)} \in \mathcal{J}_w$ and so $H = G$ by Theorem 4.3.4. □

6.6.2 Region two - $7 \leq k \leq 27$ and $m \geq 4k - 1$

Here we consider Hypothesis 6.2.7(A) and (B) simultaneously.

Lemma 6.6.6. *Let $7 \leq k \leq 28$, let $m \geq 4k-1$, and let G and M be as in Hypothesis 6.2.7. If $x \in X_1 \backslash \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. By Theorem 4.4.1, there exists a prime $p_k \geq 5$, and by Lemma 4.4.15 there exists a prime p_m such that $\frac{m}{2} < p_m \leq m-4$. Hence

$$p_m \geq \frac{m}{2} + \frac{1}{2} \geq 2k-1 \text{ and } n = mk \geq (p_m+4)k > (p_m+4)k-4, \tag{6.13}$$

and so $p_m \nmid k$ and an element with cycle type $1^{n-kp_m} \cdot p_m^k$ is in $\mathcal{J}_w$. We claim that since $x \notin \mathcal{J}$ we may assume that if $|\text{Supp}(x)| > 3k+3$. Let $y(k) = 7k^2 - 34k - 25$. Then $y(k) > 0$ for $k > 6$. Therefore

$$(3k+5)^2 = 9k^2 + 30k + 25 < 16k^2 - 4k = 4(4k-1)k$$

and so

$$3k+3 < 2\sqrt{(4k-1)k} - 2 \leq 2(\sqrt{mk}-1).$$

Thus if $|\text{Supp}(x)| \leq 3k+3$ then $x \in \mathcal{J}_s$, and so the claim holds.

Since $x \in X_1$, it follows automatically that either there exists $\alpha, \alpha^x \in \Omega_1$ or $\beta \in \Omega_1$ such that $\beta^x \notin \Omega_1 \cup \Omega_2$. Since $|\text{Supp}(x)| > 3k+3$ there exists $\gamma \in \text{Supp}(x) \backslash (\Omega_1 \cup \Omega_2 \cup \Omega_2^{x^{-1}} \cup \{\beta, \beta^x, \beta^{x^{-1}}\})$. Since $k > 3$ it follows that $2k+6 < 3k+3$ and so there exists $\delta \in \text{Supp}(x) \backslash (\Omega_2 \cup \Omega_2^{x^{-1}} \cup \{\beta, \beta^x, \beta^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}\})$. Therefore $\beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x$ are distinct points, $\beta, \beta^x, \gamma, \gamma^x, \delta, \delta^x \notin \Omega_2$ and $\gamma \notin \Omega_1$.

Let $\mathcal{Y}_1$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}})=p_m \\ \Omega_1, \Omega(\gamma), \Omega(\gamma^x), \Omega(\beta^x) \in \text{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_3^{\mathcal{M}})=m-p_m \\ \Omega_2 \in \text{Supp}(c_3^{\mathcal{M}})}}$$

with $\gamma^x \in \Theta_2$, $k+1 \in \Theta_3$ and either $\{1, \gamma, \beta, \beta^x\}$ or $\{1, \gamma, \alpha, \alpha^x\} \in \Theta_1$.

Let $\mathcal{Y}_2$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_m p_k \cdot p_m(k-p_k-1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1, \Omega(\gamma), \Omega(\gamma^x), \Omega(\delta), \Omega(\delta^x), \Omega(\beta^x) \in \text{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_4^{\mathcal{M}})=m-p_m \\ \Omega_2 \in \text{Supp}(c_4^{\mathcal{M}})}}$$

with $\gamma^x \in \Theta_2$, $\delta^x \in \Theta_3$, $k+1 \in \Theta_4$, and either $\{1, \gamma, \delta, \beta, \beta^x\}$ or $\{1, \gamma, \delta, \alpha, \alpha^x\} \in \Theta_1$.

We first show that if $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$, then $H = \langle x, y \rangle$ is primitive. Clearly H is transitive.

We claim Lemma 4.2.15 implies that H is primitive. Let $(q_1, q_2, j, \upsilon, \phi) = (p_m, p_k, 2, 1, \gamma)$, let $\psi = \omega$ be α or β, if $y \in \mathcal{Y}_1$ then let $i = 3$, otherwise let $i = 4$. Then $p_m \nmid |\Theta_i|$, $p_k \nmid |\Theta_2|$ and $p_m p_k \nmid |\Theta_l|$ for $l \geq 2$. Also $1, \gamma \in \Theta_1$, $1^x = k+1 \in \Theta_i$ and $\gamma^x \in \Theta_2$. Finally $\psi, \psi^x, \omega, \omega^x \in \Theta_1$, $\psi \in \Omega_1 \cap \Theta_1 = 1^{\langle y^{p_m} \rangle}$ and there exists $y \in \mathcal{Y}_1$ and $y \in \mathcal{Y}_2$ such that $\omega \in \gamma^{\langle y^{p_k} \rangle}$. Hence H satisfies Conditions (i), (ii) and (iii)(a) of Lemma 4.2.15, and so H is primitive.

Thus H is primitive. If $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$, then $y_1^{p_k(m-p_m)(k-p_k)k}$ and $y_2^{p_k(k-p_k-1)(m-p_m)k}$ respectively have cycle type $1^{n-p_mk} \cdot p_m^k$. Hence by (6.13) these are in $\mathcal{J}_w$. Thus $\mathrm{A}_n \leq H$ by Theorem 4.3.4. Since $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$ have different parties, it follows there exists $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$ such that $H = G$. □

6.6.3 Region six - $2 \leq m \leq 18$ and $k \geq \max\{4m-1, 28\}$

We consider 6.2.7(A) and (B) separately.

Hypothesis 6.2.7(A)

We begin with a preliminary lemma.

Lemma 6.6.7. *Let $k > 12$, let $x \in X_1 \backslash \mathcal{J}$ and let $|\mathrm{Supp}(x)| \geq 10$.*

(i) *If $\Omega_1^x \cap \Omega_1 = \emptyset$, then there exist distinct points α, α^x, β such that $\alpha \in \Omega_1 \backslash \{1\}$, $\alpha^x \notin \Omega_1 \cup \Omega_2$ and $\beta \in \Omega_2 \backslash \{k+1, 1^{x^{-1}}\}$.*

(ii) *If $\Omega_1^x \cap \Omega_1 \neq \emptyset$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \geq 4$, then exists distinct points γ, δ, δ^x such that $\gamma, \gamma^x \in \Omega_1$, $\delta \in \Omega_2 \cap \mathrm{Supp}(x)$ and $\delta, \delta^x \notin \{1, k+1, \gamma, \gamma^x\}$.*

(iii) *If $\Omega_1^x \cap \Omega_1 \neq \emptyset$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$, then there exist distinct points $\gamma, \epsilon, \zeta, \zeta^x$ such that $\gamma, \gamma^x \in \Omega_1$, $\epsilon \in \Omega_2 \cap \mathrm{Fix}(x)$ and $\zeta, \zeta^x \notin \{1, k+1, \gamma, \gamma^x\}$.*

In all cases there also exist distinct points $\eta, \eta^x \notin \{1, k+1, \alpha, \alpha^x, \beta, \gamma, \gamma^x, \delta, \delta^x, \epsilon, \zeta, \zeta^x\}$, and in addition for each $2 \leq i \leq m$, there exists $\iota_i \in \Omega_i$ such $\iota_i, \iota_i^x \notin \{1, k+1, \alpha, \alpha^x, \beta, \gamma, \gamma^x, \delta, \delta^x, \epsilon, \zeta, \zeta^x, \eta, \eta^x\}$.

Proof. (i) Since $x \in X_1$ it follows that $\Omega_1^x \neq \Omega_2$, and so if $\Omega_1^x \cap \Omega_1 = \emptyset$, then there exists $\alpha \in \Omega_1$ as required. Let $\beta \in \Omega_2 \backslash \{k+1, 1^{x^{-1}}, \alpha^{x^{-1}}\}$.

(ii)-(iii) If $\Omega_1^x \cap \Omega_1 \neq \emptyset$, then there exist $\gamma, \gamma^x \in \Omega_1$ (possibly equal). If $|\Omega_2 \cap \mathrm{Supp}(x)| \geq 4$, then there exists $\delta \in (\Omega_2 \cap \mathrm{Supp}(x)) \backslash \{k+1, 1^{x^{-1}}, \gamma^{x^{-1}}\}$. It follows automatically that $\delta \notin \{1, \gamma, \gamma^x\} \subseteq \Omega_1$, and so $\delta, \delta^x \notin \{1, k+1, \gamma, \gamma^x\}$. If $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$, then since $k > 3$ there exists $\epsilon \in \Omega_2 \backslash \mathrm{Supp}(x) \subseteq \mathrm{Fix}(x)$. Since $|\mathrm{Supp}(x)| \geq 10$ there exists $\zeta \in \mathrm{Supp}(x) \backslash \{1, k+1, 1^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}\}$ hence $\zeta, \zeta^x \notin \{1, k+1, \gamma, \gamma^x, \epsilon\}$.

Let $A = \{1, k+1, 1^{x^{-1}}, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}\}$, $\{1, k+1, 1^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}, \delta, \delta^x, \delta^{x^{-1}}\}$ or $\{1, k+1, 1^{x^{-1}}, \gamma, \gamma^x, \gamma^{x^{-1}}, \zeta, \zeta^x, \zeta^{x^{-1}}\}$, then $|A| \leq 9$. Since $|\mathrm{Supp}(x)| \geq 10$ it follows that there exists $\eta \in \mathrm{Supp}(x) \backslash A$, hence η and η^x are as required. Let $2 \leq i \leq m$, since $k > 12$ there exists $\iota_i \in \Omega_i \backslash (A \cup \{\eta, \eta^x, \eta^{x^{-1}}\})$. Hence ι_i and ι_i^x satisfy the lemma. □

Lemma 6.6.8. *Let $2 \leq m \leq 18$, let $k \geq \max\{28, 4m-1\}$, and let G and M be as in Hypothesis 6.2.7*(A). *If $x \in X_1 \backslash \mathcal{J}$, then there exists $y \in \mathcal{Y}$ such that $\langle x, y \rangle = G$.*

Proof. By Lemma 4.4.19, there exists a prime p_k such that $p_k \leq k-4$. Since $x \notin \mathcal{J}$, we may assume that $|\mathrm{Supp}(x)| \geq 10$, and so there exist points as in Lemma 6.6.7. Since $m \leq 18 < 2 \cdot 3 \cdot 5$, it follows that m has at most two proper prime divisors. If m has exactly one proper prime divisor, then denote it by q_1; and if m has two, then denote them by q_1 and q_2. Thus if $1 < d < m$ is a divisor of m then d divides either $\frac{m}{q_1}$ or $\frac{m}{q_2}$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_k m \cdot (k - p_k - 1)m \cdot m}_{l((c_1c_2c_3)^{\mathcal{M}})=m}$$

satisfying the following.

(i) $1 \in \Theta_1$, $k+1 \in \Theta_2$, $\eta \in \Theta_3$ and $\eta^x \in \Theta_1 \cup \Theta_2$.

(ii) If $\Omega_1^x \cap \Omega_1 = \emptyset$, then $\alpha \in \Theta_1$, $(k+1)^y = \alpha^x$ and $\beta, \beta^x \in \Theta_2$.

(iii) If $\Omega_1^x \cap \Omega_1 \neq \emptyset$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \geq 4$, then $\gamma, \gamma^x \in \Theta_1$. In addition the following hold.

 (a) If $\delta^x \in \Omega_1$, then $\delta, \delta^x \in \Theta_2$ and $(k+1)^{y^{-1}} = \delta^x$.

 (b) If $\delta^x \in \Omega_2$, then $\delta \in \Theta_2$ and $1^y = \delta^x \in \Theta_1$.

 (c) If $\delta^x \notin \Omega_1 \cup \Omega_2$, then $\delta \in \Theta_2$ and $1^{-y} = \delta^x \in \Theta_1$.

(iv) If $\Omega_1^x \cap \Omega_1 \neq \emptyset$ and $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$, then $\gamma, \gamma^x \in \Theta_1$ and $1^y = \epsilon \in \Theta_1$. In addition the following hold.

 (a) If $\Omega(\zeta)$, $\Omega(\zeta^x), \Omega_1, \Omega_2$ are distinct, then $(k+1)^y = \zeta$ and $\zeta^x = \zeta^y \in \Theta_2$.

 (b) If $\Omega(\zeta) = \Omega(\zeta^x)$, and if $\Omega(\zeta^x), \Omega_1, \Omega_2$ are distinct, then $(k+1)^y = \zeta \in \Theta_2$ and $\epsilon^y = \zeta^x \in \Theta_1$.

 (c) If $\zeta, \zeta^x \in \Omega_1$ or Ω_2, then let $|\{\zeta, \zeta^x\} \cap \Theta_1| = 1 = |\{\zeta, \zeta^x\} \cap \Theta_2|$.

 (d) If $\{\Omega(\zeta), \Omega(\zeta^x)\} = \{\Omega_1, \Omega_2\}$, then let $\zeta, \zeta^x \in \Theta_1$.

(v) When q_1 is defined label $\Omega_i := \Omega_1^{y^{\frac{m}{q_1}p_k}}$ and $\iota := \iota_i = 1^{y^{\frac{m}{q_1}p_k}}$, and let $\iota^x \in \Theta_1$. When q_2 is defined label $\Omega_j := \Omega_1^{y^{\frac{m}{q_2}p_k}}$ and $\kappa := \iota_j = 1^{y^{\frac{m}{q_2}p_k}}$, and let $\kappa^x \in \Theta_1$.

Since $(m, p_k) = 1$ and $1 < \frac{m}{q_2} < \frac{m}{q_1} < m$ it follows that $0, p_k, \frac{m}{q_1}p_k$ and $\frac{m}{q_2}p_k$ are distinct modulo n. Hence $\Omega_i, \Omega_j, \Omega_l, \Omega_1$ are all distinct, and so α, ι, κ are distinct. By Condition (i), $H = \langle x, y \rangle$ is transitive. Assume, by way of a contradiction, that H is an imprimitive group with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $|\Theta_1| > \frac{n}{2}$ and $p_k \nmid |\Theta_2|, |\Theta_3|$, Lemmas 4.2.14(i) and (ii) imply that $l(c_1^{\mathcal{H}}) \neq 1, p_k m$.

Let $1 < d < m$ be a divisor of m, and assume that $l(c_1^{\mathcal{H}}) = dp_k$. Then d divides $\frac{m}{q_1}$ or

$\frac{m}{q_2}$, and so Δ contains ι or κ. From $\iota^x, \kappa^x \in \Theta_1$ it follows that $\Delta^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$, and since $k+1 \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Let $e > 1$ be a divisor of m, and suppose that $l(c_1^{\mathcal{H}}) = e$. Therefore $\Omega_1 \cap \Theta_1 \subseteq \Delta$ by Lemma 4.2.13(ii). If $\Omega_1^x \cap \Omega_1 = \emptyset$, then Condition (ii) holds, and so $1, \alpha \in \Delta$ and $k+1, \alpha^x \in \Delta^x$. Now $(k+1)^y = \alpha^x$ by Condition (ii), and so $(\Delta^x)^y = \Delta^x$. Hence $\beta, \beta^x \in \Theta_2 \subseteq \Delta^x$, and so $\Delta^x = (\Delta^x)^H = \Omega$, a contradiction.

Therefore we may assume that $\Omega_1^x \cap \Omega_1 \neq \emptyset$, and so either Conditions (iii) or (iv) hold. Hence $\gamma, \gamma^x \in \Delta$, and so $\Delta^x = \Delta$ and $k+1 \in \Delta$. Since $l(c_1^{\mathcal{H}}) = e$ it follows that $\Delta^{\langle y^e \rangle} = \Delta$, and so $(\Omega_1 \cap \Theta_1) \cup (\Omega_2 \cap \Theta_2) = 1^{\langle y^e \rangle} \cup (k+1)^{\langle y^e \rangle} \subseteq \Delta$. If $|\Omega_2 \cap \mathrm{Supp}(x)| > 3$, then Condition (iii) holds. Hence $\delta \in \Omega_2 \cap \Theta_2$, and so $\delta \in \Delta$. From $\Delta^x = \Delta$ it follows that $\delta^x \in \Delta$. By Condition (iii), $\delta^x \in \Delta^y \cup \Delta^{y^{-1}}$, and so $\Delta = \Delta^H = \Omega$, a contradiction.

Hence assume that $|\Omega_2 \cap \mathrm{Supp}(x)| \leq 3$ and so Condition (iv) holds. If $\Omega(\zeta^x), \Omega_1, \Omega_2$ are distinct, then by Conditions (iv)(a) and (b) Δ^y contains $1^y = \epsilon$ and $(k+1)^y = \zeta$. Since $\epsilon \in \mathrm{Fix}(x)$ it follows that $(\Delta^y)^x = \Delta^y$, and so $\zeta^x \in \Delta^y$. By Condition (iv)(a) or (b) either $\zeta^x = \zeta^y$ or $\zeta^x = \epsilon^y$, and so $\Delta^y = (\Delta^y)^H = \Omega$, a contradiction. Hence we may assume that $\zeta, \zeta^x \in \Omega_1 \cup \Omega_2$. From $(\Omega_1 \cap \Theta_1) \cup (\Omega_2 \cap \Theta_2) \subseteq \Delta$, Conditions (iv)(c) and (d) imply that Δ contains at least one of $\{\zeta, \zeta^x\}$. Since $\Delta^x = \Delta$ it follows that $\zeta, \zeta^x \in \Delta$. Let $B := \{1, k+1, \zeta, \zeta^x\}^{\langle y^m \rangle}$, so that $B \subseteq \Delta$. By Condition (iv)(c) or (iv)(d) either $(\Omega_1 \cup \Omega_2) \cap \Theta_1$ or $(\Omega_1 \cup \Omega_2) \cap \Theta_2 \subseteq B$. Now $\Omega_1^y = \Omega_2$ implies that $\Delta = \Delta^H = \Delta$, a contradiction.

Thus H is a primitive group containing $y^{(k-p_k-1)m}$ which has cycle type $1^{n-p_k m} \cdot {p_k}^m$. Since $n = mk > m(p_k+4) - 4$ and $p_k > \frac{k}{2} > 2m - 1$ it follows that $y^{(k-p_k-1)m} \in \mathcal{J}_w$. Hence $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$. □

Hypothesis 6.2.7(B)

We begin with the following preliminary lemma.

Lemma 6.6.9. *Let $k \geq 7$, $x \in X_1 \backslash \mathcal{J}$ and $|\mathrm{Supp}(x)| \geq 9$.*

(i) *If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 3$, then there exists distinct points $\alpha, \beta \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$ such that $\alpha^x \neq 1$. If $\alpha^x, \beta^x \in \Omega_2$, then there exists $\gamma \in \Omega_1$ such that $\gamma^x \notin \Omega_2$.*

(ii) *If $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 2$, then there exist distinct points $\delta, \delta^x \in \mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2)$ and $\epsilon \in \Omega_2 \cap \mathrm{Fix}(x)$.*

In either case, for all $2 \leq i \leq m$, there exists $\zeta_i \in \Omega_i$ such that $\zeta_i, \zeta_i^x \notin \{1^{x^{-1}}, k+1, \alpha^x, \beta^x, \delta, \delta^x, \epsilon\}$.

Proof. Let $S_1 = \Omega_1 \cap \mathrm{Supp}(x)$ and $S_2 = \Omega_2 \cap \mathrm{Supp}(x)$. If $|S_1| \geq 3$, then there exists

$\alpha, \beta \in S_1 \backslash \{1\}$. By interchanging α and β if necessary, it follows that $\alpha^x \neq 1$. Since $x \in X_1$, it follows that $\Omega_1^x \neq \Omega_2$. Hence if $\alpha^x, \beta^x \in \Omega_2$, then there exists a γ as required.

If $|S_1| \leq 2$, then $|S_2| \leq 2$ since $x \in X_1$. Now $k \geq 7$ implies that there exists $\epsilon \in \Omega_2 \backslash S_2 \subseteq \mathrm{Fix}(x)$. Since $|\mathrm{Supp}(x)| \geq 9$ it follows that there exists $\delta \in \mathrm{Supp}(x) \backslash (S_1 \cup S_1^{x^{-1}} \cup S_2 \cup S_2^{x^{-1}})$. Hence $\delta, \delta^x \in \mathrm{Supp}(x) \backslash (\Omega_1 \cup \Omega_2)$.

Let $2 \leq i \leq m$. Since $k \geq 7$ there exists either $\zeta_i \in \Omega_i \backslash \{1^{x^{-1}}, 1^{x^{-2}}, k+1, \alpha^x, \beta^x\}$ or $\Omega_i \backslash \{1^{x^{-1}}, 1^{x^{-1}}, k+1, \delta, \delta^x, \delta^{x^{-1}}\}$. Since $\zeta_i \notin \Omega_1$ it follows that $\zeta_i \neq 1, \alpha, \beta$, and so $\zeta_i^x \neq k+1, \alpha^x, \beta^x$. Since $\epsilon^{x^{-1}} = \epsilon = \epsilon^x$, it follows that $\zeta_i \neq \epsilon^{x^{-1}}, \epsilon^x$. Thus ζ_i, ζ_i^x are as required. □

Lemma 6.6.10. *Let $2 \leq m \leq 18$, let $k \geq \max\{28, 4m-1\}$, and let G and M be as in Hypothesis 6.2.7*(B). *If $x \in X_1 \backslash \mathcal{J}$, then there exists $y \in \mathcal{M}$ such that $\langle x, y \rangle = G$.*

Proof. If

$$|\mathrm{Supp}(x)| < 9 < 2(\sqrt{2(28)} - 1) < 2(\sqrt{mk} - 1),$$

then $x \in \mathcal{J}_s$. Hence we may assume that $|\mathrm{Supp}(x)| \geq 9$ and let $\alpha, \beta, \gamma, \delta, \epsilon, \zeta_i$ be as in Lemma 6.6.9. By Lemma 4.4.18 there exists a prime $p_k \leq k-4$. From $m < \frac{k}{2} < p_k$, it follows that $p_k \nmid m$. Since $m \leq 18$, it follows that m has at most two distinct proper prime divisors. If m has exactly one, then denote this prime by q_1; and if m has two, then denote them by q_1 and q_2. By Lemma 4.2.1, a product of two cycles is an element of A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ with

$$\mathcal{C}(y) = \underbrace{p_k m \cdot (k - p_k)m}_{l((c_1c_2)^{\mathcal{M}})=m}$$

satisfying the following.

(i) $1 \in \Theta_1$ and $k+1 \in \Theta_2$.

(ii) If $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 3$, then $\alpha, \beta \in \Theta_1$.

  (a) If $\alpha^x, \beta^x \in \Omega_2$ and $\gamma^x \notin \Omega_1$, then $\Omega_2^y = \Omega(\gamma^x)$ and $\beta^x, \gamma, \gamma^x \in \Theta_1$.

  (b) If $\alpha^x, \beta^x \in \Omega_2$ and $\gamma^x \in \Omega_1$, then $\Omega_1^y = \Omega_2$ and $\beta^x, \gamma, \gamma^x \in \Theta_1$.

  (c) If $\alpha^x \notin \Omega_2$ or if $\beta^x \notin \Omega_2 \cup \{1\}$, then let $(k+1)^y$ be either α^x or β^x.

  (d) If $\alpha^x \in \Omega_2$ and $\beta^x = 1$, then $\Omega_1^y = \Omega_2$ and $\alpha^x \in \Theta_1$.

(iii) If $|\Omega_1 \cap \mathrm{Supp}(x)| < 3$, then $1^y = \epsilon$ and $(k+1)^y = \delta$. Hence $\Omega_1^y = \Omega_2$ and $\Omega_1^{y^2} = \Omega(\delta)$. In addition, if $\delta^x \in \Omega(\delta)$, then $\epsilon^y = \delta^x$, otherwise $\delta^x = \delta^y$. Hence in the latter case $\Omega_1^{y^3} = \Omega(\delta^x)$.

(iv) If q_1 is defined, then label $\Omega_i := \Omega_1^{y^{\frac{m}{q_1}p_k}}$ and $\zeta := \zeta_i = 1^{y^{\frac{m}{q_1}p_k}}$, and let $\zeta^x \in \Theta_1$. If q_2 is defined, then label $\Omega_j := \Omega_1^{y^{\frac{m}{q_2}p_k}}$ and $\eta := \zeta_j = 1^{y^{\frac{m}{q_2}p_k}}$, and let $\eta^x \in \Theta_1$.

(v) Label $\Omega_l := \Omega_1^{y^{p_k}}$ and $\iota := \zeta_l = 1^{y^{p_k}}$, and let $\iota^x \in \Theta_1$.

Note that Condition (ii) and (iii) never happen simultaneously. Since $(m, p_k) = 1$ and $1 < \frac{m}{q_2} < \frac{m}{q_1} < m$, it follows that $0, p_k, \frac{m}{q_1}p_k$ and $\frac{m}{q_2}p_k$ are distinct modulo n. Hence the placements of $\Omega_i, \Omega_j, \Omega_l, \Omega_1$, and so ζ, η, ι also, are well defined.

By Condition (i), $H = \langle x, y\rangle$ is transitive. Assume, by way of a contradiction, that H is a primitive group with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $|\Theta_1| > |\Theta_2|$, and $p_k \nmid |\Theta_2|$ it follows that $l(c_1^{\mathcal{H}}) \neq 1, p_k m$ by Lemma 4.2.14(i) and (ii).

Let $l(c_1^{\mathcal{H}}) = p_k$. Then by Condition (v) $1, \iota \in \Delta$ and $\iota^x \in \Theta_1$. Hence $\Delta^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$. Since $k+1 \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

If m is composite, then let $1 < d < m$ be a divisor of m and assume that $l(c_1^{\mathcal{H}}) = dp_k$. Then from $p_k \nmid |\Theta_2|$ it follows that $\Delta \subseteq \Theta_1$ by Lemma 4.2.11(iv). Now d divides either $\frac{m}{q_1}$ or $\frac{m}{q_2}$, and so either $1^{\langle y^{\frac{m}{q_1}p_k}\rangle}$ or $1^{\langle y^{\frac{m}{q_2}p_k}\rangle} \subseteq 1^{\langle y^{dp_k}\rangle} = \Delta$. Hence Δ contains either ζ or η. Since $\zeta^x, \eta^x \in \Theta_1$ it follows that $\Delta^x \in \mathrm{Supp}(c_1^{\mathcal{H}})$, and from $k+1 \in \Theta_2$ and $p_k \nmid |\Theta_2|$ we reach a contradiction by Lemma 4.2.14(iii).

Let $e > 1$ be a divisor of m and suppose that $l(c_1^{\mathcal{H}}) = e$. Then $|\Delta \cap \Theta_1| = p_k \frac{m}{e}$, and $\Omega_1 \cap \Theta_1 \subseteq \Delta$ by Lemma 4.2.13(ii). Since $p_k \nmid n$ Lemma 4.2.6 implies that $\Delta \not\subseteq \Theta_1$. Hence $y^{\mathcal{H}} = c_1^{\mathcal{H}}$, and so no H-block is fixed by y. We show that Conditions (ii) and (iii) imply a contradiction.

First assume that $|\Omega_1 \cap \mathrm{Supp}(x)| < 3$. Then $\Omega_1 \cap \Theta_1 \subseteq \Delta$ and $|\Omega_1 \cap \Theta_1| = p_k \geq 3$, imply that $\Delta^x = \Delta$. Hence $\{1, 1^x\} = \{1, k+1\} \subseteq \Delta$ and $\{1^y, (k+1)^y\} = \{\epsilon, \delta\} \subseteq \Delta^y$ by Condition (iii). Since $\epsilon \in \mathrm{Fix}(x)$ it follows that $(\Delta^y)^x = \Delta^y$, and so $\delta^x \in \Delta^y$. By Condition (iii), either $\delta^x = \epsilon^y$ or $\delta^x = \delta^y$ and so $(\Delta^y)^y = \Delta^y$, a contradiction.

Finally assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 3$. Then $1, \alpha, \beta, \gamma \in \Omega_1 \cap \Theta_1 \subseteq \Delta$. Hence $k+1, \alpha^x, \beta^x, \gamma^x \in \Delta^x$. If $\alpha^x \notin \Omega_2$ or $\beta^x \notin \Omega_2 \backslash \{1\}$, then $(\Delta^x)^y = \Delta^x$ by Condition (ii)(c), a contradiction. If $\beta^x = 1$ and $\alpha^x \in \Omega_2$, then $1 = \beta^x \in \Delta \cap \Delta^x$ by Condition (ii)(d), and so $\Delta = \Delta^x$. Since $l(c_1^{\mathcal{H}}) = e$ and $e \mid m$, it follows that $\Delta^{y^m} = \Delta$. Hence $1^{\langle y^m\rangle} \cup (\alpha^x)^{\langle y^m\rangle} = (\Omega_1 \cup \Omega_2) \cap \Theta_1 \subseteq \Delta$. Thus $\Delta^y = \Delta$ since $\Omega_1^y = \Omega_2$ by Condition (ii)(d), a contradiction. Hence we may assume that $\alpha^x, \beta^x \in \Omega_2$. Since $l(c_1^{\mathcal{H}}) = e$ and $\gamma^x, k+1 \in \Delta^x$, it follows that $\gamma^{x\langle y^m\rangle} \cup (k+1)^{\langle y^m\rangle} = (\Omega(\gamma^x) \cup \Omega_2) \cap \Theta_1 \subseteq \Delta^x$. By Condition (ii)(a) and (ii)(b), either $\Omega_2^y = \Omega(\gamma^x)$ or $\Omega(\gamma^x)^y = \Omega_2$. Therefore $(\Delta^x)^y = \Delta^x$, a contradiction.

Hence H is a primitive group and contains $y^{(k-p_k)m}$ with cycle type $1^{n-p_km} \cdot {p_k}^m$. Since $p_k > \frac{k}{2} > 2m-1$ and $n = mk > m(p_k+4)-4$, it follows that $y^{(k-p_k)m} \in \mathcal{J}_w$. Hence $\mathrm{A}_n \leq H$ by Theorem 4.3.4, and so $H = G$ by the parity of y. □

6.7 Finite regions

In this section we complete the proof of Theorem 6.1.1 by considering the remaining (finite) collection of m and k. Let m and k be as in Regions three and five of Figure 6.1.

Throughout this section we let $x \in X_2$. Hence $1^x = k+1$ and for $1 \leq i \leq m$, if $\Omega_i^x \neq \Omega_i$ then $|\Omega_1 \cap \mathrm{Supp}(x)| \geq |\Omega_i \cap \mathrm{Supp}(x)|$.

6.7.1 Region three - $7 \leq k \leq 27$ and $27 \leq m < 4k-1$

Here we consider Hypothesis 6.2.7(B) and Hypothesis 6.2.7(A) simultaneously. We begin with the case of $k = m = 27$.

Lemma 6.7.1. *Let $k = m = 27$, let G and M be as in Hypothesis 6.2.7. If $x \in X_2 \backslash \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. Since $x \notin \mathcal{J}$, we may assume that $|\mathrm{Supp}(x)| > 2(\sqrt{n}-1) = 52$. Therefore there exists $\alpha \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \{k+1\})$ and $\beta \in \mathrm{Supp}(x)\backslash(\Omega_1 \cup \{k+1, \alpha, \alpha^x, \alpha^{x^{-1}}\})$.

Let $\mathcal{Y}_1$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{27}_{\Theta_1=\Omega_1} \cdot \underbrace{20(26) \cdot 7(26)}_{l((c_2c_3)^{\mathcal{M}})=26}$$

with $1 \in \Theta_1$, $k+1 \in \Theta_2$, $\alpha \in \Theta_3$ and $\alpha^x \in \Theta_1 \cup \Theta_2$.

Let $\mathcal{Y}_2$ be the set of elements of $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{27}_{\Theta_1=\Omega_1} \cdot \underbrace{20(26) \cdot 5(26) \cdot 2(26)}_{l((c_2c_3c_4)^{\mathcal{M}})=26}$$

with $1 \in \Theta_1$, $k+1 \in \Theta_2$, $\alpha \in \Theta_3$, $\beta \in \Theta_4$ and $\alpha^x, \beta^x \in \Theta_1 \cup \Theta_2$.

Let $s \in \{1,2\}$, and for $y \in \mathcal{Y}_s$ let $H = H(y) = \langle x, y\rangle$. Then H is transitive. We show that there exists $y \in \mathcal{Y}_s$ such that H is primitive. Assume, by way of a contradiction, that H preserves, a non-trivial block Δ containing 1.

Since $l(c_1) = 3^3$, it follows by Lemma 4.2.10 that $l(c_1^{\mathcal{H}}) = 1, 3, 9$ or 27. From $3 \nmid |\Theta_i|$ for $i \neq 1$, Lemma 4.2.11(iv) implies that $\Delta \subseteq \Theta_1$. In addition, since Δ is non-trivial, it follows that $l(c_1^{\mathcal{H}}) \neq 27$. Therefore from $1^{\langle y^9\rangle} \subseteq 1^{\langle y^3\rangle} \subseteq 1^{\langle y\rangle}$, we deduce that $1^{y^9}, 1^{y^{18}} \in \Delta$. If there exist $\gamma, \gamma^x \in \Omega_1$, then there exists $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$ such that $\{\gamma, \gamma^x\} \subseteq \{1, 1^{y^9}, 1^{y^{18}}\}$. In which case $\Delta^x = \Delta$ and so $k+1 \in \Delta$, a contradiction since $\Delta \subseteq \Theta_1$. Hence we may assume that $\Omega_1^x \cap \Omega_1 = \emptyset$. Since $\Omega_1^x \neq \Omega_2$ it follows that there exists $\delta \in \Omega_1$ and $i > 2$ such that $\delta^x \in \Omega_i$. There exist $y_s \in \mathcal{Y}_s$ such that $1^{y^9} = \delta$ and $(k+1)^y = \delta^x$. Hence $k+1, \delta^x \in \Delta^x$ and so $(\Delta^x)^y = \Delta^x$. Therefore $\Theta_2 \subseteq \Delta^x$ and so $|\Delta^x| \geq 20(26) > 27 \geq |\Delta|$, a contradiction.

Thus there exist $y \in \mathcal{Y}_s$ such that $H = \langle x, y\rangle$ is primitive. Either $y^{26\cdot 20\cdot 7}$ or $y^{26\cdot 20\cdot 5\cdot 2}$ is a 27-cycle. Hence H contains an element of $\mathcal{J}_c$ and so $\mathrm{A}_n \leq H$ by Theorem 4.3.4. Therefore $H = G$ by the parity of y. □

Lemma 6.7.2. *Let $7 \leq k \leq 27$, let $27 \leq m \leq 4k-2$ and let G and M be as in Hypothesis 6.2.7. If $x \in X_2 \backslash \mathcal{J}$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. If $m = k = 27$, then the result follows by Lemma 6.7.1. Hence assume otherwise.

Since $\Omega_1^x \neq \Omega_2$, we may let $\alpha, \alpha^x \in \Omega_1$ if $\Omega_1^x \cap \Omega_1 \neq \emptyset$; and otherwise let $\beta \in \Omega_1$ such that $\beta^x \in \Omega_i$ for some $i \geq 2$.

From $k \geq 7$ it follows that $k+7 \leq 2k$ and so $k+5 \leq 2(k-1) = 2(\sqrt{k^2}-1)$ with equality if and only if $k = 7$. Since $k \leq 27$ it follows that $k \leq m$ with equality if and only if $k = 27$. Hence $k+5 < 2(\sqrt{mk}-1)$. Therefore if $|\mathrm{Supp}(x)| \leq k+5$, then $x \in \mathcal{J}_s$. Thus we may assume otherwise. Since $|\{\alpha, \alpha^x, \beta, \beta^x\}| \leq 2$, there exists either $\gamma \in \mathrm{Supp}(x) \backslash (\{1, \alpha, \alpha^x, \beta, \beta^x\} \cup \Omega_2)$ and $\delta \in \mathrm{Supp}(x) \backslash (\{1, \alpha, \alpha^x, \beta, \beta^x, \gamma, \gamma^x\} \cup \Omega_2)$. Hence $\gamma^x \neq \delta$. It can be verified in Magma, see Lemma 8.1.2 in the Appendix, that for each m and k there exist primes p_m and p_k such that $p_k \nmid (m-p_m)$, $p_m \nmid kp_k(k-p_k)$ and an element with cycle type $1^{n-p_mk} \cdot p_m^k$ is a Jordan element.

Let $\mathcal{Y}_1$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_mp_k \cdot p_m(k-p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega_i,\Omega(\gamma)\in\mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_3^{\mathcal{M}})=m-p_m \\ \Omega_2\in\mathrm{Supp}(c_3^{\mathcal{M}})}}$$

with $\gamma \in \Theta_2$, $k+1 \in \Theta_3$, $\gamma^x \in \Theta_1 \cup \Theta_3$ and either $1, \alpha, \alpha^x \in \Theta_1$ or $1, \beta, \beta^x \in \Theta_1$.

Let $\mathcal{Y}_2$ be the set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_mp_k \cdot p_m(k-p_k-1) \cdot p_m}_{\substack{l((c_1c_2c_3)^{\mathcal{M}})=p_m \\ \Omega_1,\Omega_i,\Omega(\gamma),\Omega(\delta)\in\mathrm{Supp}((c_1c_2c_3)^{\mathcal{M}})}} \cdot \underbrace{(m-p_m)k}_{\substack{l(c_4^{\mathcal{M}})=m-p_m \\ \Omega_2\in\mathrm{Supp}(c_4^{\mathcal{M}})}}$$

with $\gamma \in \Theta_2$, $\delta \in \Theta_3$, $k+1 \in \Theta_4$, $\gamma^x \in \Theta_1 \cup \Theta_4$, $\delta^x \notin \Theta_3$, and either $1, \alpha, \alpha^x \in \Theta_1$ or $1, \beta, \beta^x \in \Theta_1$.

For $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$ it is clear that $H = \langle x, y \rangle$ is transitive. We claim that H is primitive. Let $y \in \mathcal{Y}_2$, the case of $y \in \mathcal{Y}_1$ follows similarly. Suppose, by way of a contradiction, that H is an imprimitive group with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since Θ_1 contains either α, α^x or β, β^x, it follows that $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). Since $p_m p_k \nmid |\Theta_j|$ for $j \neq 1$ it follows that $l(c_1^{\mathcal{H}}) \neq p_m p_k$ by Lemma 4.2.14(ii).

If $l(c_1^{\mathcal{H}}) = p_m$, then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i). Hence Δ contains either $\{1, \alpha\}$ or $\{1, \beta\}$ and there exists $\Gamma \in \mathrm{Supp}(c_1^{\mathcal{H}})$ containing either α^x or β^x. Thus $\Delta^x = \Gamma$. Since $k+1 \in \Theta_4$ and $p_m \nmid |\Theta_4|$ we reach a contradiction by Lemma 4.2.14(iii).

If $l(c_1^{\mathcal{H}}) = p_k$, then $|\Delta \cap \Theta_1| = p_m$. Since $p_k \nmid |\Theta_i|$ for $i \neq 1$ Lemma 4.2.11(i) implies that $\Delta \subseteq \Theta_1$. Thus $|\Delta| = \pm$, a contradiction since $p_m \nmid n$.

Hence H is a primitive group. If $y \in \mathcal{Y}_1$ then $y^{p_k(k-p_k)(m-p_k)k}$; and if $y \in \mathcal{Y}_2$ then $y^{p_k(k-p_k-1)(m-p_m)k}$ has cycle type $1^{n-p_m k} \cdot p_m^k$. Hence $\mathrm{A}_n \leq H$ and so $H = G$ by the parity of y. □

6.7.2 Region five - $7 \leq m \leq 18$ and $26 \leq k < 4m - 1$

Here we deal with Hypothesis 6.2.7(A) and Hypothesis 6.2.7(B) in two separate lemmas.

Lemma 6.7.3. *Let $7 \leq m \leq 18$ and let $26 \leq k \leq 4m - 2$, and let G and M be as in Hypothesis 6.2.7*(A)*. If $x \in X_2 \backslash \mathcal{J}$, then there exists $y \in \mathcal{Y}$ such that $\langle x, y \rangle = G$.*

Proof. First let $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 2$, so that there exists $\alpha \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$. Let p_k be as in Lemma 4.4.7. Then $p_k \geq 23$, and so $p_k \nmid m(m-1)$. By Lemma 4.2.1 an element composed of three cycles is in A_n if and only if $G = \mathrm{A}_n$. Let $\mathcal{Y}$ be the set of element $y = c_1 c_2 c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_k \cdot (k - p_k)}_{\Theta_1 \cup \Theta_2 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_3^{\mathcal{M}}) = m-1}$$

with $1 \in \Theta_1$, $\alpha \in \Theta_2$, $k+1 \in \Theta_3$ and $\alpha^x \in \Theta_1 \cup \Theta_3$.

Clearly H is transitive. Assume by way of a contradiction that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$. Since $p_k \nmid m(m-1)$ it follows that $p_k \nmid n, |\Theta_2|, |\Theta_3|$. Hence Lemma 4.2.14(ii) implies that $l(c_1^{\mathcal{H}}) \neq p_k$. If $l(c_1)^{\mathcal{H}} = 1$, then $\Theta_1 \subseteq \Delta$ and so $\Delta^y = \Delta$. Since $p_k \nmid n$ it follows that $\Delta \neq \Theta_1$. Hence Δ is either $\Theta_1 \cup \Theta_2$ or $\Theta_1 \cup \Theta_3$. Since $\Theta_3 = \Omega_2 \cup \cdots \cup \Omega_m$, it follows by Lemma 4.2.14(iv) that $\mathcal{M} \backslash \{\Omega_2, \ldots, \Omega_m\} = \{\Omega_1\} \not\subseteq \mathcal{H}$, and so in particular $\Delta \neq \Theta_1 \cup \Theta_2 = \Omega_1$. Thus $\Delta = \Theta_1 \cup \Theta_3$, then $|\Delta| > \frac{n}{2}$, a contradiction. Hence H is primitive.

Since $p_k \nmid (m-1)$ it follows that $y^{(k-p_k)k(m-1)}$ is a p_k-cycle, and so $y^{(k-p_k)k(m-1)} \in \mathcal{J}_c$. Hence $H = G$ by Theorem 4.3.4.

Hence we may assume that $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$. Thus since $x \in X_2$ it follows that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. If $x = (1, k+1)$, then $x \in \mathcal{J}$. Hence we may assume that $x \neq (1, k+1)$ and let $\alpha \in \mathrm{Supp}(x) \backslash \{1, k+1\}$. Since $|\Omega_1 \cap \mathrm{Supp}(x)|, |\Omega_2 \cap \mathrm{Supp}(x)| = 1$ it follows that there exists $3 \leq i \leq m$ such that $\alpha \in \Omega_i$. By Lemma 8.1.3(i), there exists a prime $q \in \{2, 3, 5, 7, 11, 13\}$ and $p_k \geq 23$, such that $q < m$, $q \nmid (m-q)k$, and S_n and A_n are the only primitive groups of degree n containing elements with cycle type $1^{n-p_k q} \cdot {p_k}^q$. Since $p_k \geq 23$, $q \leq 13$ and $m \leq 18$, it follows that $p_k \nmid q(m-q)$.

Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}(y) = \underbrace{qp_k \cdot q(k-p_k)}_{\substack{l((c_1c_2)^{\mathcal{M}})=q \\ \Omega_1, \Omega_i \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})}} \cdot \underbrace{(m-q)k}_{\substack{l(c_3^{\mathcal{M}})=m-q \\ \Omega_2 \in \mathrm{Supp}(c_3^{\mathcal{M}})}}$$

with $1 \in \Theta_1$, $\alpha \in \Theta_2$ and $\alpha^x \in \Theta_1 \cup \Theta_3$.

Clearly H is transitive, assume by way of a contradiction that H is an imprimitive group with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, it follows that $\Omega_1 \backslash \{1\} \cap \Theta_1 \subseteq \mathrm{Fix}(x)$, and so $l(c_1^{\mathcal{H}}) \neq 1$ by Lemma 4.2.14(i). From $p_k \nmid |\Theta_2|, |\Theta_3|$ Lemma 4.2.14(ii) implies that $l(c_1)^{\mathcal{M}} \neq qp_k$.

First assume that $l(c_1^{\mathcal{H}}) = p_k$. Hence $|\Delta \cap \Omega_i \cap \Theta_1| = 1$ for all $\Omega_i \in \mathrm{Supp}(c_1^{\mathcal{M}})$. If $\Theta_1 \cap \mathrm{Supp}(x) = \{1\}$, then $\Delta^x = \Delta$ and so $k+1 \in \Delta$, a contradiction by Lemma 4.2.14(iii). If there exists $\beta \in \mathrm{Supp}(x) \backslash \{1, k+1, \alpha\}$ then $\beta \in \Omega_j$ for some $j \neq 1, 2$. Let $\mathcal{Y}_1 \subseteq \mathcal{Y}$ be the set of y for which: $\Omega_j \in \mathrm{Supp}((c_1c_2)^{\mathcal{M}})$; $1^y = \beta$; and if $\beta^x \neq 1$ then $\beta^x \in \Theta_2 \cup \Theta_3$. Hence for $y \in \mathcal{Y}_1$ it follows that $\beta \in \Delta^y$. Since $|\Delta^y \cap \Omega_1 \cap \Theta_1| = 1$, we deduce that Δ^y contains a point of $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$, and so $(\Delta^y)^x = \Delta^y$. If $\beta^x = 1$, then $\beta^{xy} = \beta$ and so $\Delta^y = (\Delta^y)^H = \Omega$, a contradiction. If $\beta^x \neq 1$ then Δ^y contains a point of Θ_2 or Θ_3, a contradiction since $p_k \nmid |\Theta_2|, |\Theta_3|$.

If $l(c_1^{\mathcal{H}}) = q$, then $\Delta \cap \Theta_1 = \Omega_1 \cap \Theta_1$ by Lemma 4.2.13(i). Hence Δ contains points of $\Omega_1 \backslash \{1\} \subseteq \mathrm{Fix}(x)$. Therefore $\Delta^x = \Delta$ and so $k+1 \in \Delta$, contradicting Lemma 4.2.14(iii) since $k+1 \in \Theta_3$ and $q \nmid |\Theta_3|$.

Hence H is primitive and contains $y^{q(k-p_k)(m-q)k}$ with cycle type $1^{n-qp_k} \cdot {p_k}^q$. Therefore H contains A_n, and so $H = G$ by the parity of y. □

Lemma 6.7.4. *Let* $7 \leq m \leq 18$, *let* $26 \leq k \leq 4m-2$, *and let* G *and* M *be as in Hypothesis 6.2.7*(B). *If* $x \in X_2 \backslash \mathcal{J}$, *then there exists* $y \in \mathcal{Y}$ *such that* $\langle x, y \rangle = G$.

Proof. Since $x \notin \mathcal{J}$ it follows that $|\mathrm{Supp}(x)| \geq 4$. First assume that $|\Omega_1 \cap \mathrm{Supp}(x)| \leq 3$. By 8.1.3(ii) there exists $p_k < k-2$ such that an element with cycle type $1^{n-mp_k} \cdot {p_k}^m$ is a Jordan element. By Lemma 6.3.10 there exists $y \in M$ such that $H = \langle x, y \rangle$ is primitive and has cycle type $1^{n-mp_k} \cdot {p_k}^m$. Hence $\mathrm{A}_n \leq H$, and so $H = G$ by the parity of y.

Finally suppose that $|\Omega_1 \cap \mathrm{Supp}(x)| \geq 4$. Let $\alpha \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1\}$ and let $\beta \in \Omega_1 \cap \mathrm{Supp}(x) \backslash \{1, \alpha, \alpha^{x^{-1}}\}$ so that $\beta^x \neq \alpha$. Let $\gamma, \delta \in \Omega_1 \backslash \{1, \alpha, \alpha^x, \alpha^{x^{-1}}, \beta, \beta^x, \beta^{x^{-1}}\}$. By Lemma 4.4.7 there exists a prime $p_k \geq 23$, and so $p_k \nmid (m-1)$. Let $\mathcal{Y}$ be a set of elements $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}(y) = \underbrace{p_k \cdot (k - p_k - 1) \cdot 1}_{\Theta_1 \cup \Theta_2 \cup \Theta_3 = \Omega_1} \cdot \underbrace{(m-1)k}_{l(c_4^{\mathcal{M}}) = m-1}$$

with $1, \gamma, \delta \in \Theta_1$, $\beta \in \Theta_2$, $\{\alpha\} = \Theta_3$, $\beta^x \in \Theta_1 \cup \Theta_4$, if $\gamma^x \in \Omega_1$ then let $\gamma^x \in \Theta_1$, and if $\delta^x \in \Omega_1$ then let $\delta^x \in \Theta_1$. Let $y \in \mathcal{Y}$ and $H = H(y) = \langle x, y \rangle$. Hence H is transitive. Suppose that H is imprimitive with non-trivial block system $\mathcal{H}$. Let $\Delta \in \mathcal{H}$ with $1 \in \Delta$.

Since $p_k \nmid |\Theta_i|$ for $i \neq 1$ it follows that $l(c_1^{\mathcal{H}}) \neq p_k$ by Lemma 4.2.14(ii). Thus by Lemma 4.2.10, $l(c_1^{\mathcal{H}}) = 1$ and $\Delta^y = \Delta$.

If Θ_1 contains γ^x or δ^x, then $\Delta^x = \Delta$, and so $\Delta = \Delta^H = \Omega$, a contradiction. Hence $\gamma^x, \delta^x \in \Theta_4 \cap \Delta^x$. If $\Omega(\gamma^x) \neq \Omega(\delta^x)$, then there exists $\mathcal{Y}_1 \subseteq \mathcal{Y}$ such that $(\gamma^x)^y = \delta^x$ for all $y \in \mathcal{Y}_1$. Thus $(\Delta^x)^y = \Delta^x$, and so $\Theta_4 \subseteq \Delta^x$. Hence $|\Delta^x| > \frac{n}{2}$, a contradiction. Therefore assume that $\Omega(\gamma^x) = \Omega(\delta^x)$. There exists $y \in \mathcal{Y}$ such that $(\gamma^x)^{y^{m-1}} = \delta^x$. Hence $(\Delta^x)^{y^{m-1}} = \Delta^x$, and so $(\gamma^x)^{\langle y^{m-1} \rangle} = \Omega(\gamma^x) \subseteq \Delta^x$ and $|\Delta^x| \geq k$. Since $|\Theta_1| \leq k$, there exists $\epsilon \in \Delta \backslash \Theta_1$. From $\Delta^y = \Delta$ it follows that $\epsilon^{\langle y \rangle} \cup \Theta_1 \subseteq \Delta$. If $\epsilon \in \Theta_4$ then Δ contains $\delta^x \in \Theta_4$. Hence $\Delta^x = \Delta$, and so $\Delta = \Delta^H = \Omega$ a contradiction. Therefore from $|\Delta| = |\Delta^x| \geq k$, it follows that $\Delta = \Theta_1 \cup \Theta_2 \cup \Theta_3 = \Omega_1$. Hence we reach a contradiction by 4.2.14(iv), since $\Theta_4 = \Omega_2 \cup \cdots \cup \Omega_m$ and $\mathcal{M} \backslash \{\Omega_2, \ldots, \Omega_m\} = \{\Omega_1\} \subseteq \mathcal{H}$.

Therefore H is a primitive group containing $y_1 = y^{(k-p_k-1)(m-1)k}$. Since $p_k \nmid (m-1)$, it follows that y_1 is a p_k-cycle, and so $y_1 \in \mathcal{J}_c$. Hence $H = G$ by Theorem 4.3.4. □

6.8 Proof of Theorems 6.1.1 and 6.1.2

In this section we complete the proof of Theorem 6.1.1 and prove Theorem 6.1.2. Recall the division of m and k into regions as illustrated in Figure 6.1.

Proof of Theorem 6.1.1. Let x be as in Proposition 6.2.8. It suffices to show that there exists $y \in M$ such that $\langle x, y \rangle = G$.

If $x \in \mathcal{J}$ then the result holds by Lemma 6.3.1. Hence assume that $x \notin \mathcal{J}$ and divide into the six regions depicted in Figure 6.1. If n is in Region one, then $2 \leq k \leq 6$ and $m \geq 23$ so the result holds by Lemmas 6.6.3 and 6.6.5. If n is as in Region two, then $7 \leq k \leq 27$ and $m \geq 4k - 1$, and the result holds by Lemma 6.6.6. If n is as in Region three then $7 \leq k \leq 27$ and $27 \leq m \leq 4k - 2$, and so the result holds by Lemma 6.7.2. If n is as in Region four, then $m \geq 19$ and $k \geq 28$ and the result holds by Propositions 6.4.1 and 6.5.1. If n is as in Region five then $7 \leq m \leq 18$ and $26 \leq k \leq 4m - 2$ and the result holds by Lemmas 6.7.3 and 6.7.4. If n is as in Region six, then $2 \leq m \leq 18$ and $k \geq \max\{4m - 1, 28\}$ the result holds by Lemmas 6.6.8 and 6.6.10. This covers all possible values of $m \geq 27$ or $k \geq 28$ as required. □

Proof of Theorem 6.1.2. If M is an intransitive subgroup, then the result follows by Theorem 5.1.1. If M is an imprimitive subgroup, then the result follows by Theorem 6.1.1.

Therefore for $G = \mathrm{A}_n$ the result holds, and it remains to consider the case $G = \mathrm{S}_n$ and $M = \mathrm{A}_n$. By [48], G is $\frac{3}{2}$-generated. Thus in particular, for all $x \in G \backslash M$ there exists $y \in G$ such that $\langle x, y \rangle = G$. The result then follows since $\langle x, y \rangle = \langle x, xy \rangle$ and either y or xy is in M. □

Chapter 7

Conclusion

Here we discuss some of further areas of interest and improvements that could be made to the work in Chapters 3, 5 and 6.

As mentioned in Section 2.2, in [47] Moscatiello and Roney-Dougal prove that for G a primitive group which is not large base, either $G = \mathrm{M}_{24}$ in its natural action on 24 points, or $\mathrm{b}(G) \leq \lceil \log n \rceil + 1$. In addition they prove that this result is optimal by showing that there are infinitely many primitive non-large-base groups with $\mathrm{b}(G) > \log n + 1$. In Theorem 3.0.3 we show that $\mathrm{I}(G) \leq 5 \log n$ and since there exist a group G with $\mathrm{I}(G) > \log n$, it follows that up to multiplication by $\frac{1}{5} < c \leq 1$ this bound is the best possible. It would be interesting to find the exact value of c and so have a result similar to that on $\mathrm{b}(G)$ in [47]. The current bounds on $\mathrm{I}(G)$ are largest when G has socle $\mathrm{PSU}_d(q)$, $\mathrm{PSp}_d(q)$ or $\mathrm{P\Omega}^{\epsilon}_d(q)$, and so improving the bounds for these groups would be a good starting place.

A tighter upper bound on $\mathrm{I}(G)$ would also improve the upper bound on $\mathrm{RC}(G)$ given in Theorem 3.0.5. As part of a joint project with S. Freedman and C.M. Roney-Dougal, we have found upper and lower bounds on $\mathrm{PSL}_d(q) \leq G \leq \mathrm{PGL}_d(q)$ acting on subspaces, and for $G = \mathrm{PSL}_d(q)$ and $\mathrm{PGL}_d(q)$ acting on 1-spaces have found the exact value $\mathrm{RC}(G)$. Another area of interest would be to find exact values or tight bounds on relational complexity of other groups.

Currently Theorem 5.1.4 holds only for primes $p \neq \frac{q^d-1}{q-1}$. Under the current restrictions on p, Theorem 5.4.1 implies that a transitive subgroup H of S_p either contains A_p or is contained in a conjugate of $\mathrm{AGL}_1(p)$. Since non-identity elements of $\mathrm{AGL}_1(p)$ fix either 0 or 1 point, it is relatively easy to test if H is contained in $\mathrm{AGL}_1(p)$. However, it also follows from Theorem 5.4.1, that to extend Theorem 5.1.4 to the case of $p = \frac{q^d-1}{q-1}$ we would need to generate transitive subgroups of S_p and show that these subgroups lie in no conjugate of $\mathrm{P\Gamma L}_d(q)$.

I am currently working on extending Theorem 6.1.1 for all $m, k \geq 2$. In particular considering the region $2 \leq m \leq 27$ and $2 \leq k \leq 28$. So far it seems that in this region M will also be a maximal coclique in $\Gamma(G)$. The smaller k is the smaller the interval $(\frac{k}{2}, k-1)$ is, and so there are fewer Bertrand primes p_k. The current proof of Theorem 6.1.1 relies on the existence of multiple Bertrand primes p_m and p_k. As a consequence, the proof for the region $2 \leq m \leq 27$ and $2 \leq k \leq 28$ will likely divide into even more cases.

Very small values of $n = mk$ can be programmed using similar code to [33, Code 1]. The number of elements in $G \backslash M$, even up to M-conjugation, grow rapidly as n grows. Therefore the current limitations of the code are $n \geq 12$. To extend Theorem 6.1.1 it would be useful to improve the efficiency of this code.

As pointed out by Prof Liebeck there are stronger results on primitive groups containing elements of prime order than those given in Section 4.3 - see for example [41]. Hopefully using some of these results will help to streamline the proofs in Chapter 6 for publication.

Chapter 8

Appendix

8.1 Small primes

In Chapters 5 and 6, we require the existence of primes with certain properties and associated Jordan elements. Here we prove there exist such primes in certain small integer ranges. In the following Lemma we find primes q_m and q_k, note that these are not Bertrand primes.

Lemma 8.1.1. *Let $m = 30$, let $28 \leq k \leq 32$ and let $n = mk$. Then there exist distinct odd primes q_m, q_k and positive integers a, b such that $q_k + a + b = k$, $q_m < m$, $q_m \nmid mk$, $q_k \nmid ab(m - q_m)k$, and either $q_m q_k \leq 2(\sqrt{n} - 1)$ or an element with cycle type $1^{n-q_m q_k} \cdot q_k^{q_m}$ is in $\mathcal{J}_w$.*

Proof. Call (q_m, q_k) *Type 1* if $q_m q_k \leq 2(\sqrt{n} - 1)$, and *Type 2* if an element with cycle type $1^{n-q_m q_k} \cdot q_k^{q_m}$ is in $\mathcal{J}_w$. The following tables gives the value of q_m, q_k, a and b for each k and the type.

k	q_m	q_k	a	b	**Type**
28	11	3	11	14	1
29	7	3	13	13	1
30	7	11	7	12	2
31	7	3	14	14	1
32	7	3	13	16	1

□

Lemma 8.1.2. *Let $7 \leq k \leq 27$, let $27 \leq m \leq 4k - 2$ with $(m, k) \neq (27, 27)$ and let $n = mk$. Then there exist primes p_k and p_m such that*

$$p_k \nmid (m - p_m), \quad p_m \nmid kp_k(k - p_k), \tag{8.1}$$

and S_n *and* A_n *are the only primitive groups of degree* n *which contain an element with cycle type* $1^{n-p_mk} \cdot p_m^k$.

Proof. We split into two cases. First suppose that m and k are not as in Table 8.1, and let $n = mk$. We show by Lagrange's Theorem that S_n and A_n are the only primitive groups containing elements of order p_m, and so the result will follow.

We prove the claim using [33, Code 4], which we summarise here. Let Y be an empty set, fix a value of k and calculate PK the set of Bertrand primes p_k. For each $27 \leq m \leq 4k-1$ calculate PM the set of primes Bertrand primes p_m. For each p_k in PK calculate a corresponding set

$$Q = \big\{p_m \in PM \;\big|\; \gcd(p_k, m-p_m) = 1 \text{ and } \gcd(p_m, k(k-p_k)p_k) = 1\big\} \subseteq PM. \quad (8.2)$$

For each $p_m \in Q$ calculate $Prim$, the set of primitive groups of degree n whose order is divisible by p_m, and if $|Prim| = 2$, then add m to Y. Hence if Y has order $4k-27$ then the result holds for this fixed value of k.

Now let m and k be as in Table 8.1, and let $n = mk$. We claim that there exist primes satisfying (8.1), such that if G is a primitive group of degree n, other than S_n or A_n, then the Sylow p_m-subgroups of G are cyclic and generated by an element whose cycle type is not $1^{n-p_mk} \cdot p_m^k$. Therefore the result will follow.

We prove the claim using [33, Code 5] which we summarise here. Let k and m be one of the possibilities in Table 8.1. We calculate PK and PM the set of Bertrand primes p_k and p_m. Let p_k be a random element of PK and calculate the corresponding set $Q \subseteq PM$ as in (8.2). We choose a random $p_m \in Q$ and calculate the set $Prim$ of primitive groups whose order is divisible by p_m. We now let $Prim2 = Prim \backslash \{\mathrm{S}_n, \mathrm{A}_n\}$. For each $G \in Prim2$ calculate $S \in \mathrm{Syl}_{p_m}(G)$ and g a generator of S. If $|S| = p_m$ and g has cycle type other than $1^{n-p_mk} \cdot p_m^k$, then the result holds for this value of k and m.

$\boldsymbol{k}$	10	13	$14,\dots,25$	21	26	27
$\boldsymbol{m}$	30	27	$2k-1, 2k+1$	30, 41, 43	30, 51, 53	53, 55

Table 8.1: Exceptions

□

Lemma 8.1.3. *Let* $7 \leq m \leq 18$, *let* $26 \leq k < 4m-1$, *and let* $n = mk$. *Then the following all hold.*

(i) *There exists* $q \in \{2,3,5,7,11,13\}$ *and* $p_k \geq 23$ *such that* $q < m$, $q \nmid (m-q)k$, *and*

S_n *and* A_n *are the only primitive groups of degree* n *which contain an element with cycle type* $1^{n-p_k q} \cdot {p_k}^q$.

(ii) *There exists* $p_k < k-2$ *such that* S_n *and* A_n *are the only primitive groups of degree* n *which contain an element with cycle type* $1^{n-p_k m} \cdot {p_k}^m$.

Proof. The methods here are very similar to those of Lemma 8.1.2. First assume that m and k are not in Table 8.2. Then [33, Code 21] shows that there exist p_k and q as described such that S_n and A_n are the only primitive groups of degree n whose order is divisible by p_k.

Let m and k be as in Table 8.2. Then [33, Code 22] shows that there exists p_k and q as described such any primitive group of degree n, other than S_n and A_n, has cyclic Sylow p_k-subgroups which are generated by an element whose cycle structure is neither $1^{n-p_k q} \cdot {p_k}^q$ nor $1^{n-p_k m} \cdot {p_k}^q$.

$\boldsymbol{m}$	10	13	$14, \ldots, 18$
$\boldsymbol{k}$	30	27	$2k-1, 2k+1$

Table 8.2: Exceptions

□

8.2 Small cases of Theorem 5.1.1

Recall Notation 5.2.1 and Hypothesis 5.2.5 - let $n > k > \frac{n}{2} \geq 6$ and let $\Omega = \Omega_1 \cup \Omega_2 = \{1, \ldots, k\} \cup \{k+1, \ldots, n\}$. Let $G = \mathrm{S}_n$ or A_n acting on Ω, let

$$M = \mathrm{Stab}_G(\Omega_1) = \mathrm{Stab}_G(\Omega_2) \cong \Big(\mathrm{S}_k \times \mathrm{S}_{n-k}\Big) \cap G,$$

and let $x \in G \backslash M$. Let $\mathcal{J}_t, \mathcal{J}_c$ and $\mathcal{J}_s$ be as in Definition 4.3.3, and let $\mathcal{J}$ be as in Theorem 4.3.4.

Here we prove three useful elementary lemmas that help to simplify the proof of Theorem 5.1.1. We show, under particular restrictions on n and $x \in G \backslash M$, that either $x \in \mathcal{J}$ or there exists $y \in M$ such that $\langle x, y\rangle = G$.

For clearer exposition, in the following lemmas we omit fixed points in cycle type notation. So, for example, in place of $1^{n-5} \cdot 2 \cdot 3$ we write $2 \cdot 3$.

Lemma 8.2.1. *Let* $n \geq 12$, G, M *and* x *be as in Hypothesis 5.2.5. If* $|\mathrm{Supp}(x)| \leq 11$ *then either* $x \in \mathcal{J}$ *or*

$$\mathcal{C}(x) \in T_1 := \{2^3,\ 2^4,\ 2^5,\ 3^2,\ 3^3,\ 4^2,\ 4^2 \cdot 2,\ 5^2,\ 6 \cdot 2,\ 6 \cdot 2^2,\ 6 \cdot 3 \cdot 2,\ 6 \cdot 3,\ 8 \cdot 2,\ 10,\ 11\}.$$

Proof. Using ConjugacyClasses(Sym(11)) in MAGMA we find the 56 possible cycle structures of elements with support at most 11 (i.e. all partitions of $s \leq 11$). Since $|T_1| = 15$, and by Hypothesis 5.2.5 x is neither the identity or a transposition, there are 39 cycle structures left to consider. We show that every element with one of these cycle structures is in $\mathcal{J}$.

If

$$\mathcal{C}(x) \in \begin{cases} U_1 := \{3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}, \\ U_2 := \{2\cdot 3,\ 2^2\cdot 3,\ 2^3\cdot 3,\ 2^4\cdot 3,\ 2\cdot 5,\ 2^2\cdot 5,\ 2^3\cdot 5,\ 2\cdot 7,\ 2^2\cdot 7,\ 2\cdot 9\}, \\ U_3 := \{2\cdot 3^2,\ 2\cdot 3^3,\ 3\cdot 4,\ 3^2\cdot 4,\ 3\cdot 5,\ 3^2\cdot 5,\ 3\cdot 7,\ 3\cdot 8\}, \\ U_4 := \{3\cdot 4^2,\ 2\cdot 3\cdot 4,\ 2^2\cdot 3\cdot 4,\ 2\cdot 4\cdot 5,\ 4\cdot 5,\ 4\cdot 7\},\ \text{or} \\ U_5 := \{2\cdot 3\cdot 5,\ 5\cdot 6\} \end{cases}$$

then x, x^2, x^3, x^4 or x^6 respectively is in $\mathcal{J}_c$.

If

$$\mathcal{C}(x) \in \begin{cases} U_6 := \{2^2\} \\ U_7 := \{2\cdot 4,\ 2^2\cdot 4,\ 2^3\cdot 4\}, \\ U_8 := \{2^2\cdot 3^2\},\ \text{or} \\ U_9 := \{4\cdot 6\} \end{cases}$$

then x, x^2, x^3 or x^6 respectively is in $\mathcal{J}_t$.

Since $U_1, \dots, U_9$ are pairwise disjoint, and $\sum_{i=1}^{9} |U_i| = 39$ the result follows. □

Lemma 8.2.2. *Let n, G, M and x be as in Hypothesis 5.2.5, and assume that $|\mathrm{Supp}(x)| \leq 11$ and*

$$\mathcal{C}(x) \notin T_2 := \{2^5,\ 4^2,\ 4^2\cdot 2,\ 5^2,\ 6\cdot 2,\ 6\cdot 2^2,\ 6\cdot 3\cdot 2,\ 6\cdot 3,\ 8\cdot 2,\ 10,\ 11\}.$$

Then either $x \in \mathcal{J}$ or there exists an element $y \in M$ such that $\langle x, y\rangle = G$.

Proof. By Lemma 8.2.1 if $\mathcal{C}(x) \notin T_1$ then $x \in \mathcal{J}$. Hence it remains to consider

$$T_3 : = T_1 \backslash T_2 = \{2^3,\ 3^2,\ 2^4,\ 3^3\}.$$

First suppose that $\mathcal{C}(x) = 2^3$. Then x is odd, and so $G = \mathrm{S}_n$. If $n \geq 16$ then $|\mathrm{Supp}(x)| = 6 \leq 2(\sqrt{n}-1)$, and so $x \in \mathcal{J}_s$. Recall that $n \geq 12$ by Hypothesis 5.2.5, so we may assume that $12 \leq n \leq 15$. For these remaining cases we consider the possibilities for x and $n-k$.

By Lemmas 4.1.7 and 5.2.2 we may assume that x is one of the following.

$$
\begin{aligned}
x_1 &= (1,k+1)(2,3)(4,5) & x_4 &= (1,k+1)(2,3)(k+2,k+3)\\
x_2 &= (1,k+1)(2,3)(4,k+2) & x_5 &= (1,k+1)(2,k+2)(k+3,k+4)\\
x_3 &= (1,k+1)(2,k+2)(3,k+3) & x_6 &= (1,k+1)(k+2,k+3)(k+4,k+5)
\end{aligned}
$$

Since $12 \leq n \leq 15$, it follows that $1 \leq n-k \leq 7$. Some of $x_1, \dots, x_6$ are only defined for $n-k$ suitably large, for example x_5 requires $n-k \geq 4$. For each possible value of $n-k$ we give the corresponding possibilities for k and the maximum value of i for which $x_1, \dots, x_i$ are well defined.

$\boldsymbol{n-k}$	1	2	3	4	5	6	7
$\boldsymbol{k}$	11-14	10-13	9-12	8-11	7-10	7-9	8
$\boldsymbol{i}$	1	2	4	5	6	6	6

We then use [33, Code 7] in Magma, which tests elements of M at random to see if they are suitable choices of y. In each case we find $y \in M$ such that $\langle x, y \rangle = G$.

We now carry out the same method for the remaining cycle structures. In each case Lemmas 4.1.7 and 5.2.2 imply that it suffices to consider the following possibilities for k, $n-k$ and x. The result then follows by [33, Code 7].

If $\mathcal{C}(x) = 3^2$, then $G = \mathrm{S}_n$ or A_n. If $n \geq 16$ then $x \in \mathcal{J}_s$. Hence we may assume that $n \leq 15$ and we have the following possibilities for x, $n-k$ and k.

$$
\begin{aligned}
x_1 &= (1,k+1,2)(3,4,5) & x_5 &= (1,k+1,2)(k+2,k+3,3)\\
x_2 &= (1,k+1,k+2)(2,3,4) & x_6 &= (1,k+1,k+2)(k+3,k+4,2)\\
x_3 &= (1,k+1,2)(k+2,3,4) & x_7 &= (1,k+1,2)(k+2,k+3,k+4)\\
x_4 &= (1,k+1,k+2)(k+3,2,3) & x_8 &= (1,k+1,k+2)(k+3,k+4,k+5)
\end{aligned}
$$

$\boldsymbol{n-k}$	1	2	3	4	5	6	7
$\boldsymbol{k}$	11-14	10-13	9-12	8-11	7-10	7-9	8
$\boldsymbol{i}$	1	3	5	7	8	8	8

If $\mathcal{C}(x) = 2^4$, then $G = \mathrm{S}_n$ or A_n. If $n \geq 25$ then $x \in \mathcal{J}_s$. Hence we may assume that $n \leq 24$ and we have the following possibilities for x, $n-k$ and k.

$$
\begin{aligned}
x_1 &= (1,k+1)(2,3)(4,5)(6,7) & x_6 &= (1,k+1)(k+2,k+3)(k+4,2)(3,4)\\
x_2 &= (1,k+1)(k+2,2)(3,4)(5,6) & x_7 &= (1,k+1)(k+2,k+3)(k+4,2)(k+5,3)\\
x_3 &= (1,k+1)(k+2,k+3)(2,3)(4,5) & x_8 &= (1,k+1)(k+2,k+3)(k+4,k+5)(2,3)\\
x_4 &= (1,k+1)(k+2,2)(k+3,3)(4,5) & x_9 &= (1,k+1)(k+2,k+3)(k+4,k+5)(k+6,2)\\
x_5 &= (1,k+1)(k+2,2)(k+3,3)(k+4,4) & x_{10} &= (1,k+1)(k+2,k+3)(k+4,k+5)(k+6,k+7)
\end{aligned}
$$

$\boldsymbol{n-k}$	1	2	3	4	5	6	7	8	9	10	11
$\boldsymbol{k}$	11-23	10-22	9-21	8-20	7-19	7-18	8-17	9-16	10-15	11-14	12-13
$\boldsymbol{i}$	1	2	4	6	8	9	10	10	10	10	10

If $\mathcal{C}(x) = 3^3$, then $G = \mathrm{S}_n$ or A_n. If $n \geq 31$ then $x \in \mathcal{J}_s$. Hence we may assume that $n \leq 30$ and we have the following possibilities for x, $n-k$ and k.

$$\begin{aligned}
x_1 &= (1, k+1, 2)(3, 4, 5)(6, 7, 8)\\
x_2 &= (1, k+1, k+2)(2, 3, 4)(5, 6, 7)\\
x_3 &= (1, k+1, 2)(k+2, 3, 4)(5, 6, 7)\\
x_4 &= (1, k+1, k+2)(k+3, 2, 4)(4, 5, 6)\\
x_5 &= (1, k+1, 2)(k+2, k+3, 3)(4, 5, 6)\\
x_6 &= (1, k+1, 2)(k+2, 3, 4)(k+3, 5, 6)\\
x_7 &= (1, k+1, k+2)(k+3, k+4, 2)(3, 4, 5)\\
x_8 &= (1, k+1, k+2)(k+3, 2, 3)(k+4, 4, 5)\\
x_9 &= (1, k+1, 2)(k+2, k+3, k+4)(3, 4, 5)\\
x_{10} &= (1, k+1, 2)(k+2, k+3, 3)(k+4, 4, 5)\\
x_{11} &= (1, k+1, k+2)(k+3, k+4, k+5)(2, 3, 4)\\
x_{12} &= (1, k+1, k+2)(k+3, k+4, 2)(k+5, 3, 4)\\
x_{13} &= (1, k+1, 2)(k+2, k+3, k+4)(k+5, 3, 4)\\
x_{14} &= (1, k+1, 2)(k+2, k+3, 3)(k+4, k+5, 4)\\
x_{15} &= (1, k+1, k+2)(k+3, k+4, k+5)(k+6, 2, 3)\\
x_{16} &= (1, k+1, k+2)(k+3, k+4, 2)(k+5, k+6, 3)\\
x_{17} &= (1, k+1, 2)(k+2, k+3, k+4)(k+5, k+6, 3)\\
x_{18} &= (1, k+1, k+2)(k+3, k+4, k+5)(k+6, k+7, 2)\\
x_{19} &= (1, k+1, 2)(k+2, k+3, k+4)(k+5, k+6, k+7)\\
x_{20} &= (1, k+1, k+2)(k+3, k+4, k+5)(k+6, k+7, k+8)
\end{aligned}$$

$\boldsymbol{n-k}$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\boldsymbol{k}$	11-29	10-28	9-27	8-26	7-25	7-24	8-23	9-22	10-21	11-20	12-19	13-18	14-17	15-16
$\boldsymbol{i}$	1	3	6	10	14	17	19	20	20	20	20	20	20	20

□

Lemma 8.2.3. *Let n, G, M, and x be as in Hypothesis 5.2.5. If $n-k \leq 10$ and $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then either $x \in \mathcal{J}$ or there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. From $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ and $n-k \leq 10$, it follows that $|\mathrm{Supp}(x)| \leq 11$.

By Lemma Lemma 8.2.2 the result holds if $x \notin T_2$. Since $|\Omega_1| = k > \frac{n}{2} > 6$, it follows that x fixes at least 5 points. Hence if x a cycle, then $x \in \mathcal{J}_c$. Therefore we may assume that

$$\mathcal{C}(x) \in T_4 := T_2 \backslash \{10, 11\} = \{2^5,\ 4^2,\ 4^2 \cdot 2,\ 5^2,\ 6 \cdot 2,\ 6 \cdot 2^2,\ 6 \cdot 3,\ 6 \cdot 3 \cdot 2,\ 8 \cdot 2\}$$

Therefore by Lemmas 4.1.7 and 5.2.2 we may assume that x is one of the following.

$$\begin{aligned}
x_1 =&(1, k+1)(k+2, k+3)(k+4, k+5)(k+6, k+7)(k+8, k+9)\\
x_2 =&(1, k+1, k+2, k+3)(k+4, k+5, k+6, k+7)\\
x_3 =&(1, k+1)(k+2, k+3, k+4, k+5)(k+6, k+7, k+8, k+9)\\
x_4 =&(1, k+1, k+2, k+3)(k+4, k+5, k+6, k+7)(k+8, k+9)\\
x_5 =&(1, k+1, k+2, k+3, k+4)(k+5, k+6, k+7, k+8, k+9)\\
x_6 =&(1, k+1)(k+2, k+3, k+4, k+5, k+6, k+7)\\
x_7 =&(1, k+1, k+2, k+3, k+4, k+5)(k+6, k+7)\\
x_8 =&(1, k+1)(k+2, k+3)(k+4, k+5, k+6, k+7, k+8, k+9)\\
x_9 =&(1, k+1, k+2, k+3, k+4, k+5)(k+6, k+7)(k+8, k+9)\\
x_{10} =&(1, k+1, k+2)(k+3, k+4, k+5, k+6, k+7, k+8)\\
x_{11} =&(1, k+1, k+2, k+3, k+4, k+5)(k+6, k+7, k+8)\\
x_{12} =&(1, k+1)(k+2, k+3, k+4)(k+5, k+6, k+7, k+8, k+9, k+10)\\
x_{13} =&(1, k+1, k+2)(k+3, k+4)(k+5, k+6, k+7, k+8, k+9, k+10)\\
x_{14} =&(1, k+1, k+2, k+3, k+4, k+5)(k+6, k+7)(k+8, k+9, k+10)\\
x_{15} =&(1, k+1)(k+2, k+3, k+4, k+5, k+6, k+7, k+8, k+9)\\
x_{16} =&(1, k+1, k+2, k+3, k+4, k+5, k+6, k+7)(k+8, k+9)
\end{aligned}$$

We now introduce two equations which bound the possibilities for n and $n-k$. If $x \in \mathcal{J}_s$ then the lemma holds. Hence assume that $x \notin \mathcal{J}_s$ and so $2(\sqrt{n}-1) < |\mathrm{Supp}(x)|$. Therefore

$$n \leq \left\lceil \left(\frac{1}{2}|\mathrm{Supp}(x)| + 1\right)^2 \right\rceil - 1. \tag{8.3}$$

Recall that $n-k < \frac{n}{2}$, and so $n-k \leq \frac{n-1}{2}$. Additionally, by assumption, $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ and $n-k \leq 10$, thus

$$|\mathrm{Supp}(x)| - 1 \leq n-k \leq \min\left\{10, \frac{n-1}{2}\right\}. \tag{8.4}$$

Using (8.3) and (8.4) we calculate the possibilities for $n-k$ and k, and then proceed via Magma.

If $x \in \{x_2, x_6, x_7\}$, then $|\mathrm{Supp}(x)| = 8$. Hence $n \leq 24$ by (8.3), and $7 \leq n-k \leq 10$ by (8.4). Therefore we need to consider the following values of $n-k$ and k.

$\boldsymbol{n-k}$	7	8	9	10
$\boldsymbol{k}$	8-17	9-16	10-15	11-14

If $x \in \{x_{10}, x_{11}\}$, then $|\mathrm{Supp}(x)| = 9$. Hence $n \leq 30$ by (8.3), and $8 \leq n-k \leq 10$ by (8.4). Therefore we need to consider the following values of $n-k$ and k.

$\boldsymbol{n-k}$	8	9	10
$\boldsymbol{k}$	9-22	10-21	11-20

If $x \in \{x_1, x_3, x_4, x_5, x_8, x_9, x_{15}, x_{16}\}$, then $|\mathrm{Supp}(x)| = 10$. Hence $n \leq 35$ by (8.3), and $9 \leq n-k \leq 10$ by (8.4). Therefore we need to consider the following values of $n-k$ and k.

$\boldsymbol{n-k}$	9	10
$\boldsymbol{k}$	10-26	11-25

If $x \in \{x_{12}, x_{13}, x_{14}\}$, then $|\mathrm{Supp}(x)| = 11$. Hence $n \leq 42$ by (8.3), and $10 \leq n-k \leq 10$ by (8.4). Therefore we need to consider $n-k = 10$ and $11 \leq k \leq 32$.

For each x, k and $n-k$ we use [33, Code 6], which tests random elements of M, to find $y \in M$ such that $\langle x, y\rangle = G$. □

Lemma 8.2.4. *Let n, G, M and x be as in Hypothesis 5.2.5. If $k \leq 9$ and $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$ then either $x \in \mathcal{J}$ or there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. It is immediate from Hypothesis 5.2.5 that $7 \leq k \leq 9$ and $12 \leq n \leq 17$. Our assumption that $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$, implies that $|\mathrm{Supp}(x)| \leq k+1 \leq 10$.

By Lemma 8.2.2 the result holds if $x \notin T_2$. Therefore we may assume that

$$\begin{aligned}\mathcal{C}(x) \in T_4 :&= \{\mathcal{C}(x) \in T_2 \mid |\mathrm{Supp}(x)| \leq 10\}\\ &= \{2^5,\ 4^2,\ 4^2 \cdot 2,\ 5^2,\ 6 \cdot 2,\ 6 \cdot 2^2,\ 6 \cdot 3,\ 8 \cdot 2,\ 10\}\end{aligned}$$

Therefore by Lemmas 4.1.7 and 5.2.2 we may assume that x is one of the following (where we list the possibilities for x with support increasing).

$$\begin{aligned}
x_1 &= (1, k+1, 2, 3)(4, 5, 6, 7) & x_8 &= (1, k+1)(2, 3, 4, 5)(6, 7, 8, 9)\\
x_2 &= (1, k+1, 2, 3, 4, 5)(6, 7) & x_9 &= (1, k+1, 2, 3, 4)(5, 6, 7, 8, 9)\\
x_3 &= (1, k+1)(2, 3, 4, 5, 6, 7) & x_{10} &= (1, k+1, 2, 3, 4, 5)(6, 7)(8, 9)\\
x_4 &= (1, k+1, 2, 3, 4, 5)(6, 7, 8) & x_{11} &= (1, k+1)(2, 3, 4, 5, 6, 7)(8, 9)\\
x_5 &= (1, k+1, 2)(3, 4, 5, 6, 7, 8) & x_{12} &= (1, k+1, 2, 3, 4, 5, 6, 7)(8, 9)\\
x_6 &= (1, k+1)(2, 3)(4, 5)(6, 7)(8, 9) & x_{13} &= (1, k+1)(2, 3, 4, 5, 6, 7, 8, 9)\\
x_7 &= (1, k+1, 2, 3)(4, 5, 6, 7)(8, 9) & x_{14} &= (1, k+1, 2, 3, 4, 5, 6, 7, 8, 9)
\end{aligned}$$

The following gives the possibilities for k and $n-k$, and the corresponding maximum values of i for which $x_1, \ldots, x_i$ are defined.

$\boldsymbol{k}$	7	8	9
$\boldsymbol{n-k}$	$5, 6$	$4, \ldots, 7$	$3, \ldots, 8$
$\boldsymbol{x_i}$	3	5	14

For each G and x we use [33, Code 9] in Magma. This shows that by choosing sufficiently many random elements of M, we find $y \in M$ such that $\langle x, y \rangle = G$. □

Bibliography

[1] K.D. Blaha, *Minimum bases for permutation groups: the greedy approximation.* J. Algorithms 13 (1992), no. 2, 297–306.

[2] N. Bourbaki, *Groupes et Algebrès de Lie* (Chapters 4,5 and 6), Hermann, Paris (1968).

[3] J.N. Bray, D.F. Holt, C.M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups.* Lond. Math. Soc. Lect. Note Ser., 407. Cambridge University Press, Cambridge, 2013.

[4] T.C. Breuer, R.M. Guralnick, A. Lucchini, A. Maróti and G.P. Nagy, *Hamiltonian cycles in the generating graphs of finite groups.* Bull. Lond. Math. Soc. 42 (2010), no. 4, 621–633.

[5] T.C. Burness, *On base sizes for actions of finite classical groups.* J. Lond. Math. Soc. (2) 75 (2007), no. 3, 545–562.

[6] T.C. Burness, *On base sizes for almost simple primitive groups.* J. Algebra 516 (2018), 38–74.

[7] T.C. Burness and M. Giudici, *Classical groups, derangements and primes.* Volume 25 of Aust. Math. Soc. Lect. Ser. Cambridge: Cambridge University Press, 2016.

[8] T.C. Burness, R.M. Guralnick and S. Harper, *The spread of a finite group*, arXiv:2006.01421, 2020.

[9] T.C. Burness and S. Harper, *On the uniform domination number of a finite simple group.* Trans. Amer. Math. Soc. 372 (2019), no. 1, 545–583.

[10] T.C. Burness and S. Harper, *Finite groups, 2-generation and the uniform domination number.* Israel J. Math. 239 (2020), no. 1, 271–367.

[11] T.C. Burness, M. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron.* Proc. Lond. Math. Soc. (3) 98 (2009), no. 1, 116–162.

[12] T.C. Burness, M. Liebeck and A. Shalev, *Generation and random generation: from simple groups to maximal subgroups.* Adv. Math. 248 (2013), 59-95.

[13] T.C. Burness, E. O'Brien and R. Wilson, *Base sizes for sporadic simple groups.* Israel J. Math. 177 (2010), 307–333.

[14] P.J. Cameron, A. Lucchini and C.M. Roney-Dougal, *Generating sets of finite groups.* Trans. Amer. Math. Soc. 370 (2018), no. 9, 6751–6770.

[15] P.J. Cameron, P.M. Neumann and D.N. Teague, *On the degrees of primitive permutation groups.* Math. Z. 180 (1982), no. 2, 141–149.

[16] P.J. Cameron, R. Solomon and A. Turull, *Chains of subgroups in symmetric groups* J. Algebra 127 (1989), no. 2, 340–352.

[17] P. Chebyshev, *Memoire sur les nombres premiers.* Journal de mathematiques pures et appliquees (1852), no. 17, 366-390.

[18] G. Cherlin, *Sporadic homogeneous structures.* The Gelfand Mathematical Seminars, 1996–1999, 15–48, Gelfand Math. Sem., Birkhäuser Boston, Boston, MA, 2000.

[19] G. Cherlin, G. Martin and D. Saracino, *Arities of permutation groups: wreath products and k-sets.* J. Combin. Theory Ser. A 74 (1996), no. 2, 249–286.

[20] J. H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, $\mathbb{ATLAS}$ *of finite groups. Maximal subgroups and ordinary characters for simple groups.* Oxford University Press, Eynsham, 1985.

[21] E. Crestani and A. Lucchini, *The non-isolated vertices in the generating graph of a direct powers of simple groups.* J. Algebraic Combin. 37 (2013), no. 2, 249–263.

[22] D. Cvetković, *Graphs and their spectra.* Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz. No. 354–356 (1971), 1–50.

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

[24] K. Doerk and T.O. Hawkes, *Finite Soluble Groups.* De Gruyter Expositions in Mathematics, 4. Walter de Gruyter & Co., Berlin, 1992.

[25] M. Garonzi and A. Lucchini, *Maximal irredundant families of minimal size in the alternating group.* Arch. Math. (Basel) 113 (2019), no. 2, 119–126.

[26] N. Gill, M. Liebeck and P. Spiga, *Cherlin's conjecture on finite primitive binary permutation groups.* arXiv:2106.05154.

[27] N. Gill and B. Lodá, *Statistics for* S_n *acting on k-sets.* arXiv:2101.08644.

[28] N. Gill, B. Lodá and P. Spiga, *On the height and relational complexity of a finite permutation group.* Nagoya Math. J, to appear.

[29] R.M. Guralnick and W. Kantor, *Probabilistic generation of finite simple groups.* J. Algebra 234, 743–792 (2000).

[30] Z. Halasi, M.W. Liebeck and A. Maroti, *Base sizes of primitive groups: bounds with explicit constants* arXiv:1802.06972.

[31] G.A. Jones, *Primitive permutation groups containing a cycle.* Bull. Aust. Math. Soc. 89 (2014), no. 1, 159–165.

[32] C. Jordan, *Sur la limite de transitivite des groupes non alteres*, Bull. Sot. Math. France 1 (1873), 40-71.

[33] V. Kelsey and C.M. Roney-Dougal, *Magma Code* `https://veronicakelsey.github.io`

[34] V. Kelsey and C.M. Roney-Dougal, *A Maximal Coclique in* A_n *and* S_n arXiv:2007.12021

[35] V. Kelsey and C.M. Roney-Dougal, *On relational complexity and base size of finite primitive groups.* arXiv:2107.14208

[36] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, volume 129 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1990.

[37] A. Lachlan, *On countable stable structures which are homogeneous for a finite relational language.* Israel J. Math. 49 (1984), no. 1-3, 69-153.

[38] M.W. Liebeck, *On minimal degrees and base sizes of primitive permutation groups.* Arch. Math., 43:11–15, 1984.

[39] M.W. Liebeck, C.E. Praeger and J. Saxl *A classification of the maximal subgroups of the finite alternating and symmetric groups.* J. Algebra 111 (1987), no. 2, 365-383.

[40] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces.* Proc. London Math. Soc. (3) 63 (1991), no. 2, 266–314.

[41] M.W. Liebeck and J. Saxl, *Primitive permutation groups containing an element of large prime order.* J. London Math. Soc. (2) 31 (1985), no. 2, 237–249.

[42] M.W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky.* J. Algebra 184 (1996), no. 1, 31–57.

[43] B. Lodá, *The height and relational complexity of finite permutation groups.* PhD Thesis, University of South Wales, 2020.

[44] A. Lucchini and A. Maróti, *On the clique number of the generating graph of a finite group* Proc. Amer. Math. Soc. 137 (2009), no. 10, 3207–3217.

[45] A. Lucchini and A. Maróti, *Some results and questions related to the generating graph of a finite group.* In: Ischia group theory 2008, World Sci. Publ., Hackensack, NJ, 2009, pp. 183–208.

[46] W.A. Manning, *On the order of primitive groups, I-II,* Trans. Amer. Math. Sot. 10 (1909), 247-258; 16 (1915), 139-147; 19 (1918), 127-142.

[47] M. Moscatiello and C.M. Roney-Dougal, *Base size of primitive permutation groups.* Monatsh. Math, to appear.

[48] S. Piccard, *Sur les bases du groupe symètrique et du groupe alternant*, Math. Ann. 116 (1939), 752-767.

[49] B.J. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. 6 (1962), 64–94.

[50] J. Saunders, *Maximal cocliques in* $\mathrm{PSL}_2(q)$. Comm. Algebra 47 (2019), no. 10, 3921–3931.

[51] C.C. Sims, *Computation with finitely presented groups.* Encyclopedia of Mathematics and its Applications, 48. Cambridge University Press, Cambridge, 1994.

[52] R. Steinberg, *Generators for simple groups.* Canadian J. Math. 14 (1962), 277–283.

[53] L. Stringer, *Pairwise Generating Sets for the Symmetric and Alternating Groups* PhD Thesis, Royal Holloway University of London, 2008.

[54] M. Suzuki, *Group theory. I.* Translated from the Japanese by the author. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 247. Springer-Verlag, Berlin-New York, 1982.

[55] D.E. Taylor, *The geometry of the classical groups.* Sigma series in pure mathematics. Heldermann Verlag, 1992.

[56] P. Turan, *An extremal problem in graph theory,* Mat. Fiz, Lapok 48 (1941), 436-452.

[57] A.V. Vasilyev, *Minimal permutation representations of finite simple exceptional groups of types E_6, E_7 and E_8.* Alg. and Logic 36, 302-310 (1997).

[58] H. Wielandt, *Finite permutation groups.* Translated from the German by R. Bercov Academic Press, New York-London 1964.