Pairwise Generating Sets for the Symmetric and Alternating Groups

Linda Stringer

Technical Report
RHUL–MA–2009–14
23 April 2009

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

PAIRWISE GENERATING SETS FOR THE SYMMETRIC AND ALTERNATING GROUPS

Linda Stringer

Royal Holloway,
University of London

Thesis submitted to

The University of London

for the degree of

Doctor of Philosophy

2008.

Declaration

I, Linda Stringer, declare that the work presented in this thesis is my own.

Abstract

For all sufficiently large odd integers n, there exists a set of 2^{n-1} permutations that pairwise generate the symmetric group S_n, and there is no larger set having this property. This was proved by Blackburn in 2006. He proved a similar result for A_n, that is, for all sufficiently large even integers n such that $n \equiv 2 \pmod 4$, there exists a set of 2^{n-2} permutations that pairwise generate the symmetric group A_n, and there is no larger set having this property. We give explicit versions of these results. We prove that the result for S_n holds for all odd integers n except for $5, 9$ and possibly 15. We prove that the result for A_n holds for all even integers n such that $n \equiv 2 \pmod 4$, except for 6 and possibly $10, 14$ and 18.

For $n \geq 21$, our proofs extend and refine the proofs given by Blackburn; we use a similar probabilistic method. Whereas those proofs use an asymptotic upper bound for the number of conjugacy classes of primitive maximal subgroups of S_n, we determine and use an explicit upper bound. Also, we develop theory concerning imprimitive maximal subgroups of S_n which we use in `GAP` programs, and we use detailed information about primitive maximal subgroups of S_n which we obtain from the `GAP` data library. For $n < 21$ we use constructive proofs.

We also answer the following question of Maróti in the affirmative: For all sufficiently large integers n, does there exist a set of n^3 permutations that pairwise generate A_n ? In fact we prove a stronger result for most values of n.

Acknowledgements

I would like to thank my supervisor Professor Simon Blackburn for his encouragement and inspiration over the last three years.

Thankyou to my fellow students and staff at Royal Holloway for their friendliness and support.

Finally, thankyou to my family for their enthusiasm, and for their help and patience while I have been busy with this thesis.

Contents

List of Tables

Chapter 1

Introduction

In this chapter we present our main theorem, and discuss an important property of a pairwise generating set of order 2^{n-1} for S_n, when n is odd. We also describe the structure of this thesis.

1.1 Our main theorem

Let G be a finite group that can be generated by two elements. We say that a subset $X \subseteq G$ *generates* G *pairwise* if for all $g_1, g_2 \in X$ with $g_1 \neq g_2$ we have that g_1, g_2 generate G. We write $\mu(G)$ for the largest order of a set that generates G pairwise.

Blackburn proved in 2006 that for all sufficiently large odd integers n, we have $\mu(S_n) = 2^{n-1}$, and that for all sufficiently large even integers n with $n \equiv 2 \pmod 4$ we have $\mu(A_n) = 2^{n-2}$ [2]. In this thesis we prove the following.

Theorem 1.1.1. *Let n be a positive integer.*

1. *If n is odd and $n \neq 5$, 9, or 15, then $\mu(S_n) = 2^{n-1}$.*
2. *We have $\mu(S_5) = 13 < 16 = 2^{5-1}$ and $235 \leq \mu(S_9) \leq 244 < 256 = 2^{9-1}$.*
3. *If $n \equiv 2 \pmod 4$, and $n \neq 6$, 10, 14, or 18, then $\mu(A_n) = 2^{n-2}$.*
4. *We have $\mu(A_6) = 11 < 16 = 2^{6-2}$.*

We also answer the following question of Maróti in the affirmative: Is $\mu(A_n) \geq n^3$ for all but finitely many values of n ? We actually prove a stronger result.

1.2 A covering and a pairwise generating set

If X generates G pairwise, then no distinct pair of elements of X is contained in a proper subgroup of G. That is

$$|X \cap H| \leq 1 \text{ for all } H < G.$$

Equivalently, no distinct pair of elements of X is contained in a maximal subgroup of X. We say that a set $\mathcal{L}$ of proper subgroups of G is a *covering* if G is the set-theoretic union of the subgroups in $\mathcal{L}$, and then since

$$|X \cap H| \leq 1 \text{ for all } H \in \mathcal{L},$$

the order of any pairwise generating set is less than the number of subgroups in any covering. In 1994, Cohn defined $\sigma(G)$ to be the least integer m such that G is the union of m of its proper subgroups [4], so $\sigma(G)$ is the minimal number of subgroups in a covering of G. It follows that $\mu(G) \leq \sigma(G)$.

Let n be an odd integer, and let $\mathcal{L}$ be the set of all intransitive maximal subgroups of S_n, together with A_n. There is a one-one correspondence between the intransitive maximal subgroups of S_n and the partitions of the set $\Omega = \{1, \ldots, n\}$ into two non-empty subsets, that is the two orbits of the subgroup, Δ and $\Omega \setminus \Delta$ say, are the parts of the corresponding partition. Since n is odd there are precisely $2^{n-1} - 1$ intransitive maximal subgroups of S_n (corresponding to the $2^{n-1} - 1$ partitions of the set $\Omega = \{1, \ldots, n\}$ into precisely two subsets), so $|\mathcal{L}| = 2^{n-1}$.

An element of S_n which has only one orbit on Ω is an n-cycle. Since n is odd, an n-cycle is an even permutation and so is an element of A_n. Any element g of S_n which has two or more orbits on Ω is contained in at least one of the intransitive maximal subgroups of S_n, for suppose that g has orbits $\Delta_1, \ldots, \Delta_r$ on Ω, then g is contained in the intransitive maximal subgroup which has orbits Δ_1 and $\Delta_2 \cup \ldots \cup \Delta_r$. Therefore $\mathcal{L}$ is a covering for S_n. It follows that $\sigma(S_n) \leq 2^{n-1}$ and so $\mu(S_n) \leq 2^{n-1}$.

(In 2005, Maróti proved for odd integers $n > 3$, that if $n \neq 9$, then $\mathcal{L}$ is in fact a minimal covering so $\sigma(S_n) = 2^{n-1}$ [18]. He also proved that if $n \equiv 2 \pmod 4$, then $\sigma(A_n) = 2^{n-2}$.)

In order to prove that $\mu(S_n) \geq 2^{n-1}$, we use the covering $\mathcal{L}$ as a starting point to try to find a pairwise generating set for S_n of order 2^{n-1}. Suppose that X is such a set. Then

$$|X \cap H| = 1 \text{ for all } H \in \mathcal{L}.$$

Furthermore, since $|X| = |\mathcal{L}|$, each element of X must be contained in only one of the subgroups in $\mathcal{L}$. An element g of S_n which has three or more orbits on Ω is contained in more than of the subgroups in $\mathcal{L}$, for suppose that g has orbits $\Delta_1, \ldots \Delta_r$ on Ω, then g is contained in both the intransitive maximal subgroup which has orbits Δ_1 and $\Delta_2 \cup \ldots \cup \Delta_r$, and that which has orbits $\Delta_1 \cup \ldots \cup \Delta_{r-1}$ and Δ_r (these are not the same because $r \geq 3$.) Therefore each element of X must have at most two orbits on Ω. Since n is odd, an element g of S_n which has two orbits on Ω is not contained in A_n, for then g is the product of two disjoint cycles, one of which is of odd length and one of which is of even length, so g is not an even permutation. An element of S_n which has only one orbit on Ω is an n-cycle and is contained in A_n, and so X must contain exactly one n-cycle. The remaining $2^{n-1} - 1$ elements of X must therefore each have two orbits on Ω, and this pair of orbits must be different for each element (because each element must be contained in a different intransitive maximal subgroup.) This is certainly always possible, since there are $2^{n-1} - 1$ partitions of the set Ω into precisely two subsets.

However, this is not sufficient to ensure that X generates S_n pairwise, as if $n > 3$, then S_n has many more maximal subgroups to consider. We must ensure that

$$|X \cap H| \leq 1 \text{ for all } H < S_n,\ H \notin \mathcal{L},$$

that is, no other maximal subgroup of S_n (one not in $\mathcal{L}$) contains more than one element of X.

We prove that $\mu(S_n) \geq 2^{n-1}$ for most values of n by extending and refining the probabilistic method of Blackburn; we prove that a pairwise generating set of order 2^{n-1} exists, without actually constructing such a set. This proof requires an explicit (but not tight) upper bound for the number of conjugacy classes of primitive maximal subgroups of S_n. It also requires a detailed study of the imprimitive maximal subgroups of S_n. For $n \in \{7, 11, 13, 17, 19\}$ we give a constructive proof of the existence of a pairwise generating set for S_n of order 2^{n-1}, for $n = 3$ and we actually give the pairwise generating sets for S_3 of order $4 = 2^{3-1}$. We study the awkward cases $n = 5$ and 9. The results for A_n where $n \equiv 2 \pmod 4$ are proved using a similar combination of probabilistic and constructive methods.

1.3 The structure of this thesis

Following preliminaries in Chapter 2, as a gentle introduction in Chapter 3 we give constructive proofs and consider $\mu(S_n)$ for some small values of n. In Chapter 4 we give an overview of our proof for S_n using the probabilistic method, in order to motivate Chapters 5, 6, and 7 which are on probabilities, imprimitive maximal subgroups of S_n and primitive maximal subgroups of S_n respectively. These chapters provide the results necessary for our actual proof using the probabilistic method which is given in Chapter 8. We consider $\mu(A_n)$ where $n \equiv 2 \pmod 4$ in Chapter 9, and finally in Chapter 10 we address the question of Maróti. We include ten appendices, the first of which is a pairwise generating set for S_9, and the remaining nine are computer programs.

Chapter 2

Preliminaries

This chapter contains a collection of definitions, notation, preliminary results, and well known theorems, organised into two sections - group theory and combinatorics.

2.1 Group theory

2.1.1 Group actions and permutation groups

Let G be a group and let X be an non-empty set. Suppose that there is a map $a : X \times G \to X$ which satisfies $a(x, 1_G) = x$, and $a(a(x, g), h) = a(x, gh)$ for all $x \in X$ and $g, h \in G$. Then we say that this map defines an *action* of G on X. Following the usual convention, we write x^g for $a(x, g)$, thus the conditions above become

$$x^{1_G} = x$$

$$(x^g)^h = x^{gh}$$

for all $x \in X$ and $g, h \in G$.

The set of permutations of X under composition is a group called the *symmetric group* on X and is denoted by $\mathrm{Sym}(X)$. A *permutation group* is any subgroup of a symmetric group, and any subgroup of $\mathrm{Sym}(X)$ acts on X in an obvious way (as well as sometimes in a less obvious way, as we shall see). For a positive integer n, we let Ω be the set $\Omega = \{1, \ldots, n\}$ we use S_n for the symmetric group $\mathrm{Sym}(\Omega)$, and we use A_n for the alternating group $\mathrm{Alt}(\Omega)$. We use e for the identity element 1_{S_n} of S_n.

An action of G on X allows us to define a homomorphism of G into $\mathrm{Sym}(X)$, in the following way. Define $\phi : G \to \mathrm{Sym}(X)$ by letting $\phi(g)$ be the map $\phi(g) : X \to X$, defined by $\phi(g) : x \mapsto x^g$ for all $x \in X$ and $g \in G$. Now for each $g \in G$, the map $\phi(g)$ is clearly a well defined map from X to X, and it is injective because if $\phi(g)[x] = \phi(g)[y]$ for some $x, y \in X$, then $x^g = y^g$, $(x^g)^{g^{-1}} = (y^g)^{g^{-1}}$ and $x = y$, by the definition of a group action. So indeed $\phi(g) \in \mathrm{Sym}(X)$. The map ϕ is a group homomorphism because for all $x \in X$ and $g, h \in G$ we have

$$x^{[\phi(g)\phi(h)]} = [x^{\phi(g)}]^{\phi(h)} = (x^g)^{\phi(h)} = (x^g)^h = x^{gh} = x^{[\phi(gh)]}.$$

The homomorphism ϕ is called the *permutation representation* of the action of G on X. The *kernel* of the action is the kernel of the permutation representation, that is $g \in G$ such that $\phi(g) = 1_{\mathrm{Sym}(X)}$, or equivalently $g \in G$ such that $x^g = x$ for all $x \in X$. An action is called *faithful* if $\ker \phi = 1_G$, in which case G is isomorphic to the image of its permutation representation in $\mathrm{Sym}(X)$. An action is *transitive* if for all $x, y \in X$ there exists $g \in G$ such that $x^g = y$, and the action is *intransitive* otherwise.

We give a useful faithful and transitive action of G on itself. Let $g \in G$ and for all h in G let $h^g = hg$, that is g acts on all the elements of G by right multiplication. We call the permutation representation of this action the *right regular representation* of G. Thus for each $g \in G$ we have an image $\widehat{g} \in \mathrm{Sym}(G)$ which is the map $\widehat{g} : h \mapsto hg$.

Two actions of an abstract group, G, on sets X and Y, are *equivalent* if there exists a bijection $\psi : X \to Y$ such that

$$[\psi(x)]^g = \psi(x^g) \text{ for all } x \in X \text{ and } g \in G.$$

For $g, h \in G$, we say that g is conjugate to h if $g = k^{-1}hk$ for some $k \in G$.

We define the *conjugacy class* containing g,

$$[g]_G = \{k^{-1}gk \mid k \in G\},$$

and if $H \leq G$ we define the *conjugacy class of subgroups*

$$[H]_G = \{k^{-1}Hk \mid k \in G\}.$$

For $x \in X$, we define the *point stabiliser*

$$G_x = \{g \in G \mid x^g = x\}.$$

The set of point stabilisers of a transitive action of G is a conjugacy class of subgroups of G, and if faithful transitive actions of G on X and Y are equivalent, then each action has the same conjugacy class of point stabilisers.

2.1.2 Permutation isomorphism

Two permutation groups, say $G \leq \mathrm{Sym}(X)$ and $H \leq \mathrm{Sym}(Y)$ are *permutation isomorphic* if there exists a group isomorphism $\phi : G \to H$, and a bijection $\psi : X \to Y$ such that

$$[\psi(x)]^{\phi(g)} = \psi(x^g) \text{ for all } x \in X \text{ and } g \in G.$$

If an abstract group G acts faithfully on a set X, then G (acting in this way) is *permutation isomorphic* to the image $\phi(G)$ of the permutation representation ϕ of this action in $\mathrm{Sym}(X)$ (acting in the obvious way on X.) The necessary isomorphism is simply the permutation representation ϕ, and the bijection is the identity map, and we have by definition

$$x^{\phi(g)} = x^g \text{ for all } x \in X \text{ and } g \in G.$$

Hereafter we do not specify which action of a group we are talking about, if it is completely clear from the context (in particular, a permutation group acts in the obvious way, unless stated otherwise).

If an abstract group G acts faithfully on a set X of order n, then G is *permutation isomorphic* to a subgroup of S_n. We let ψ be any bijection $\psi : X \to \Omega = \{1, \ldots, n\}$ and define an equivalent action of G on Ω by $[\psi(x)]^g = \psi(x^g)$. We let $\sigma : G \to S_n$ be the permutation representation of this action. Then G is permutation isomorphic to $\sigma(G) < S_n$ and σ and ψ are the necessary isomorphism and bijection respectively, since

$$[\psi(x)]^{\sigma(g)} = \psi(x^g).$$

Different bijections from X to Ω define in this way conjugate subgroups of S_n, as we now explain. Let ψ_1 and ψ_2 be bijections from X to Ω and let σ_1 and σ_2 be the corresponding isomorphisms, and let $g \in G$. Then for all $x \in X$ we have $\psi_1^{-1}([\psi_1(x)]^{\sigma_1(g)}) = x^g = \psi_2^{-1}([\psi_2(x)]^{\sigma_2(g)})$. Let $\pi = \psi_1\psi_2^{-1} \in S_n$. Then for all $x \in X$ we have $[\psi_1(x)]^{\sigma_1(g)} = \psi_1\psi_2^{-1}([\psi_2(x)]^{\sigma_2(g)}) = \pi([\pi^{-1}\psi_1(x)]^{\sigma_2(g)}) = [\psi_1(x)]^{\pi^{-1}\sigma_2(g)\pi}$. Therefore $\sigma_1(g) = \pi^{-1}\sigma_2(g)\pi$, so $\sigma_1(G)$ and $\sigma_2(G)$ are conjugate subgroups of S_n. We say that an element g of G *induces* the element $\sigma(g)$ of S_n.

Lemma 2.1.1. *Two subgroups of S_n are permutation isomorphic if and only if they are conjugate.*

Proof. Let $G \leq S_n$, and suppose that G is permutation isomorphic to a subgroup $\phi(G)$, where ϕ is the permutation isomorphism and ψ is the bijection such that $[\psi(\omega)]^{\phi(g)} = \psi(\omega^g)$ for all $\omega \in \Omega$ and $g \in G$. Then since $\psi \in S_n$, we write this as $[(\omega)^\psi]^{\phi(g)} = (\omega^g)^\psi$ for all $\omega \in Omega$, so $\psi\phi(g) = g\psi$ and $\phi(g) = \psi^{-1}g\psi$. Thus G is conjugate to $\phi(G)$.

Conversely, let $G \leq S_n$, and let $\psi \in S_n$. Then let ϕ be the homomorphism $\phi : G \to G$ defined by $\phi : g \mapsto \psi^{-1}g\psi$ for all $g \in G$. Then ϕ is a permutation isomorphism and ψ the associated bijection since $[\psi(\omega)]^{\phi(g)} = [\omega^\psi]^{\psi^{-1}g\psi} = \omega^{g\psi} = \psi[\omega^g]$. □

When an abstract group G acts faithfully with degree n, we have shown that G acting in this way is permutation isomorphic to all the subgroups in a conjugacy class of subgroups of S_n. We often simply say that the abstract group G is a subgroup of S_n, when we are actually referring to one of the subgroups of S_n which is permutation isomorphic to G acting in a way which is clear from the context. Also, we call the subgroups in the conjugacy class *copies* of G in S_n. For example we refer to the subgroup $S_2 \times S_3$ of S_5, when we mean a subgroup of S_5 which is permutation isomorphic to $S_2 \times S_3$ acting intransitively with degree 5, or we discuss the copies of $S_2 \times S_3$ in S_5.

If faithful actions of G on X and Y are equivalent, then they are permutation isomorphic. However, the converse is not true in general. We give an example to illustrate this point.

Example 2.1.1. The symmetric group S_6 has two faithful degree 6 actions which are permutation isomorphic but not equivalent. The first is the usual action on $\{1, \ldots, 6\}$. The point stabilisers of this action are the intransitive subgroups, S_5. The second action is the right multiplication action of S_6 on the right cosets of a transitive subgroup which is isomorphic to S_5. (This transitive subgroup is itself the image in S_6 of a permutation representation of the transitive conjugation action of S_5 on its six Sylow-5 subgroups.) This transitive subgroup is a point stabiliser of this second action, and is certainly not one of the point stabilisers of the first action. For further details see [20, Section 2.4.3].

It is important to make the distinction between isomorphism, permutation isomorphism and equivalence. Sometimes when we are talking about isomorphism we say *(abstract group) isomorphism*, in order to emphasise that we are not talking about permutation isomorphism.

An abstract group G acts on itself by conjugation. Let $g \in G$ and for all h in G let $h^g = g^{-1}hg$. For each $g \in G$, the image $\mathrm{Inn}(g) \in \mathrm{Sym}(G)$ of the permutation representation of this action is not only a permutation of G, it is an automorphism, so we have $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) < \mathrm{Sym}(G)$. Automorphisms which arise in this way are called *inner automorphisms*, and any other automorphism of G is an *outer automorphism*.

It is interesting to note that if there are two faithful transitive actions of degree n an abstract group G which are permutation isomorphic, but not equivalent, then the permutation isomorphism ϕ from G to G must be an outer automorphism of G. For if the permutation isomorphism ϕ were an inner automorphism, then conjugacy class of point stabilisers of the actions would be the same, and the actions would be equivalent. Moreover, the outer automorphism ϕ must not stabilise setwise each of the conjugacy classes of core free index n subgroups of G (again, because actions are equivalent if and only if the set of point stabilisers is the same). In our example above, the permutation isomorphism is indeed an outer automorphism of S_6.

Lemma 2.1.2. *Let G be a finite group, and let n be a positive integer.*

1. *There is a one-one correspondence between faithful transitive actions of G of degree n, up to equivalence, and core-free index n subgroups of G, up to conjugacy.*

2. *There is a one-one correspondence between faithful transitive actions of G of degree n, up to permutation isomorphism, and subgroups of S_n which are isomorphic to G, up to conjugacy.*

3. *The number of conjugacy classes of transitive subgroups of S_n which are isomorphic to G is at most the number of conjugacy classes of core-free index n subgroups of G.*

4. *The number of conjugacy classes of transitive subgroups of S_n which are isomorphic to G is at most the number of faithful transitive actions of G of degree n, up to equivalence.*

Proof. 1. Suppose that G acts faithfully and transitively with degree n. The set of point stabilisers is a conjugacy class of index n subgroups of G. These subgroups are core-free because the action is faithful. Two equivalent such actions of G define the same conjugacy class, because equivalent actions have the same set of point stabilisers.

Conversely, given a conjugacy class $[H]_G$ of core-free index n subgroups of G, the right coset action of G on the set of cosets $[G : H]$ is a transitive action, which is faithful because H is core-free. Using the set of cosets $[G : K]$ of a different representative, $K = g^{-1}Hg$ say, gives an equivalent action: let $\psi : [G : H] \to [G : K]$ be defined by $\psi : Hx \mapsto Kg^{-1}x$, then

$$[\psi(Hx)]y = [Kg^{-1}x]y = Kg^{-1}(xy) = \psi[H(xy)] = \psi[(Hx)y].$$

2. Suppose that G acts faithfully and transitively on a set X of order n. We have described above how G is permutation isomorphic to the subgroups in a conjugacy class of subgroups which are isomorphic to G. Clearly any other action which is permutation isomorphic to this action of G on X is permutation isomorphic to the same conjugacy class of subgroups of S_n.

Conversely, given a transitive subgroup G of S_n, then G acts faithfully and transitively on Ω (in the obvious way). By Lemma 2.1.1, the (obvious) action of any other representative (on Ω), of the conjugacy class $[G]_{S_n}$ is permutation isomorphic to this action.

3. and 4. If two actions of a group G are equivalent then they are certainly permutation isomorphic, but the converse to this does not hold in general. Thus the number of actions of G up to permutation isomorphism is at most the number of such actions up to equivalence. Parts 3 and 4 then follow from parts 1 and 2 above. $\square$

2.1.3 Products and semi-direct products of groups

Let G and H be groups. We obtain another group called the *direct product* $G \times H$ which has elements and product operation

$$G \times H = \{(g, h) : g \in G, h \in H\},$$
$$(g, h)(x, y) = (gx, hy).$$

It follows that $1_{G\times H} = (1_G, 1_H)$ and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

If there is a homomorphism $\phi : H \to Aut(G)$, we obtain the *semi-direct product* $G :_\phi H$ (or $G \rtimes H$) associated with this homomorphism which has elements and product operation

$$G :_\phi H = \{(g, h) : g \in G, h \in H\},$$
$$(g, h)(x, y) = (gx^{\phi(h^{-1})}, hy).$$

It follows that $1_{G:_\phi H} = (1_G, 1_H)$ and $(g, h)^{-1} = (g^{-1\phi(h^{-1})}, h^{-1})$. It is necessary that $\phi(h)$ is an automorphism of G for each $h \in H$ to ensure that this product is associative. $G :_\phi H$ has subgroups $G^* = G \times \{1_H\}$ and $H^* = (1_G) \times H$ which are isomorphic to G and H respectively. The action by conjugation of H^* on G^* is permutation isomorphic to the action of H on G since

$$(1, h)^{-1}(g, 1)(1, h) = (1, h^{-1})(g, h) = (g^{\phi(h)}, 1).$$

(This would not be true without the inverse in the definition of the product.)

The *wreath product* $G \wr H$ is a particular type of semi-direct product. If G and H are permutation groups, say $G \leq S_l$ and $H \leq S_m$, then there is a homomorphism $\phi : H \to \mathrm{Aut}(G^m)$, defined as follows. For $h \in H$, and $(g_1, \dots, g_m) \in G^m$, let

$$\phi(h) : (g_1, \dots, g_m) \mapsto (g_{1^{h^{-1}}}, \dots, g_{m^{h^{-1}}}).$$

Then $\phi(h)$ is an automorphism of G^m (without the inverse this would not be true). G^m is called the base group, and the *wreath product* $G \wr H$ is simply the semi-direct product $G^m :_\phi H$.

2.1.4 Maximal subgroups of the symmetric and alternating groups

Suppose that the action of a group G on a set X is transitive and $\mathcal{B} = \{B_1, \ldots, B_k\}$ is a partition of X into (disjoint) subsets such that $B_i^g \in \mathcal{B}$ for all i and all $g \in G$. Then $\mathcal{B}$ is a *system of blocks* for G. The action of G is *primitive* if no such (non-trivial) system exists, and is *imprimitive* otherwise.

Therefore a subgroup of S_n is either intransitive, (transitive) imprimitive, or (transitive) primitive. The O'Nan Scott theorem classifies maximal subgroups of S_n and A_n, and here we give this theorem as it is described in [13]

Theorem 2.1.3 (The O'Nan-Scott theorem)**.** *Let n be a positive integer. If X is A_n or S_n, and G is any maximal subgroup of X with $G \neq A_n$, then G satisfies one of the following:*

1. $G = (S_m \times S_k) \cap X$, *with* $n = m + k$ *and* $m \neq k$ (intransitive case)*;*

2. $G = (S_m \wr S_k) \cap X$, *with* $n = mk$, $m > 1$, $k > 1$ (imprimitive case)*;*

3. $G = \mathrm{AGL}(k, p) \cap X$, *with* $n = p^k$ *and p prime* (affine case)*;*

4. $G = (T^k.(\mathrm{Out}(T) \times S_k)) \cap X$, *$T$ nonabelian simple,* $k \geq 2$, $|T|^{k-1} = n$ (diagonal case)*;*

5. $G = (S_m \wr S_k) \cap X$, *with* $n = m^k$, $m \geq 5$, $k > 1$, *excluding the case where* $X = A_n$ *and G is imprimitive on* Ω (wreath case)*;*

6. $T \triangleleft G \leq \mathrm{Aut}(T)$, *$T$ nonabelian simple,* $T \neq A_n$ *and G acting primitively* (almost simple case)*.*

Although it is not explicitly mentioned, maximal subgroups in parts 3 to 6 of this theorem are (transitive and) primitive. Not all subgroups in these classes are maximal. The main theorem in [13] tells us that if G is a subgroup of S_n in classes 1 to 5, then G is maximal in A_nG, and if G is a subgroup of A_n in classes 1 to 5, then G is maximal in A_n except for five exceptions (which occur when $n = 7, 8, 11, 17$ and 23). An explicit list of exceptions to maximality is given for subgroups in class 6.

We give a lemma which provides the order of a conjugacy class of subgroups.

Lemma 2.1.4. *Let an abstract group G act faithfully and transitively with degree n, and suppose that (when considering G as a subgroup of S_n), G is a maximal subgroup of S_n other than A_n. Then S_n contains $n!/|G|$ copies of G.*

Proof. Let σ be the permutation representation of an equivalent action of G on Ω, and let $M = \sigma(G)$ so $|M = |G|$. Then $[M]_{S_n}$ is the set of copies of G in S_n, and S_n acts on the set of subgroups $[M]_{S_n}$ by conjugation. In this action, the stabiliser of the subgroup M is the normaliser $N_{S_n}(M)$ of M in S_n, and certainly contains M. We have $M \leq N_{S_n}(M) \leq S_n$. Since $M \neq A_n$, we know that $N_{S_n}(M) \neq S_n$. Then by maximality of M, the stabiliser $N_{S_n}(M)$ must be M itself. The action is also transitive. Then by the Orbit-Stabiliser Theorem, $|[M]_{S_n}| \times |N_{S_n}(M)| = |S_n|$, so $|[M]_{S_n}| = n!/|G|$. □

We give some further notation, and then a lemma concerning the affine maximal subgroups. Suppose that a permutation $g \in S_n$ consists of r disjoint cycles of lengths $l_1, l_2, \ldots, l_r$, where $l_1, l_2, \ldots, l_r$ are positive integers such that $1 \leq l_1 \leq l_2 \leq \ldots \leq l_r$ and $l_1 + l_2 + \ldots + l_r = n$. Then g has r disjoint orbits on Ω (some of which may be trivial orbits of length 1), and we say that g is a $(l_1, l_2, \ldots, l_r)$-cycle. Usually if $l_1 = \ldots = l_s = 1$ for some $s < r$, we simply say that g is a $(l_{s+1}, \ldots, l_r)$-cycle (that is we omit the cycles of length 1), and if g is a (t)-cycle, we say that g is a t-cycle (we drop the brackets). For example, the element $(1234) \in S_4$ is a 4-cycle and has one orbit on $\Omega = \{1, 2, 3, 4\}$, the element $(123)(4) \in S_4$ is a $(1, 3)$-cycle or a 3-cycle and has two orbits on Ω (of which one is trivial), and the element $(12)(34) \in S_4$ is a $(2, 2)$-cycle and has two orbits on Ω. If $r = 2$ we sometimes say that g is a *bi-cycle.*

If $n = p^d$ for a prime p, then $\mathrm{AGL}(d,p)$ is a maximal subgroup of S_n. So if $p > 3$ is prime $\mathrm{AGL}(1,p)$ is a maximal subgroup of S_p, and we use this fact in the following lemma. We use φ to denote the Euler's totient function, that is $\varphi(n)$ is the number of integers that are less than n and are co-prime to n, for example $\varphi(6) = 2$, since 1 and 5 are co-prime to 6.

Lemma 2.1.5. *Let p be an odd prime. Each copy of $\mathrm{AGL}(1,p)$ in S_p contains exactly $p\,\varphi(p-1)$ elements which are $(p-1)$-cycles, and each of the p distinct copies of S_{p-1} in S_p contains exactly $\varphi(p-1)$ of these $(p-1)$-cycles. Also any fixed $(p-1)$-cycle is contained in exactly $\varphi(p-1)$ of the $(p-2)!$ copies of $\mathrm{AGL}(1,p)$.*

Proof. $\mathrm{AGL}(1,p)$ is the group of affine transformations of a vector space of dimension 1 over $\mathbb{Z}_p$ under composition. Therefore $\mathrm{AGL}(1,p) = \{T_{a,b} : a \in \mathbb{Z}_p \setminus 0, b \in \mathbb{Z}_p\}$, where $T_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ is defined by $T_{a,b} : x \mapsto ax + b$, for all $x \in \mathbb{Z}_p$. It is isomorphic to the semidirect product $\mathbb{Z}_p \rtimes GL(1,p)$, so $|\mathrm{AGL}(1,p)| = |\mathbb{Z}_p| \times |GL(1,p)| = p(p-1) = p^2 - p$. Now $\mathrm{AGL}(1,p)$ contains a cyclic normal subgroup of order p (which consists of the transformations $\{T_{1,b} : b \in \mathbb{Z}_p\}$), and p cyclic subgroups of order $(p-1)$ which are not normal (for example $\{T_{a,0} : a \in \mathbb{Z}_p \setminus 0\}$. Clearly $\mathrm{AGL}(1,p)$ as a maximal subgroup of S_p has the same structure. It has a single cyclic normal subgroup of order p, which contains $(p-1)$ elements which are p-cycles. It also has p cyclic subgroups of order $(p-1)$. These are conjugate by the p-cycles. They each fix a different point of $\{1, 2, \ldots, p\}$ and are contained in the p different copies of S_{p-1} in S_p. Pairwise they intersect trivially, and the non-trivial elements of these subgroups account for the other $p(p-2)$ elements of $\mathrm{AGL}(1,p)$ (therefore all elements of $\mathrm{AGL}(1,p)$ are elements of cyclic groups of order p or $(p-1)$). Now a cyclic group of order $(p-1)$ contains exactly $\varphi(p-1)$ elements which are $(p-1)$-cycles, and so $\mathrm{AGL}(1,p)$ contains exactly $p\varphi(p-1)$ elements which are $(p-1)$-cycles.

Now we count pairs (h, H) in two ways, where H is any copy of $\mathrm{AGL}(1, p)$ and h is any $(p-1)$-cycle in H. Let r be the number of such pairs.

First we have $r = xy$, where x is the number of $(p-1)$-cycles in S_p, and y is the number of copies of $\mathrm{AGL}(1, p)$ which contain a fixed $(p-1)$-cycle. This number is independent of the choice of cycle, since all $(p-1)$-cycles and all copies of $\mathrm{AGL}(1, p)$ are conjugate in S_p. Then $x = p\,(p-2)!$, and y is the number we wish to find out, and $r = p\,(p-2)!\,y$.

Second we have $r = zw$, where z is the number of $(p-1)$-cycles in any fixed copy of $\mathrm{AGL}(1, p)$ (again, this number is independent of the choice of copy), and w is the number of copies of $\mathrm{AGL}(1, p)$ in S_p. We have already shown that $z = p\varphi(p-1)$, and by maximality of $\mathrm{AGL}(1, p)$ in S_p, we have $w = p!/|\mathrm{AGL}(1, p)| = (p-2)!$. So $r = p\,\varphi(p-1)\,(p-2)!$.

Equating our two expressions for r gives us $p\,(p-2)!\,y = p\,\varphi(p-1)\,(p-2)!$, so $y = \varphi(p-1)$ which means that any fixed $(p-1)$-cycle is contained in $\varphi(p-1)$ copies of $\mathrm{AGL}(1, p)$. □

2.1.5 Simple groups

A group G is *simple* if the only normal subgroups of G are the trivial subgroup $\{1_G\}$ and G itself. We first state a theorem from [11], known as the power order theorem, that tells us that there are at most two finite simple groups of a given order (up to isomorphism).

Theorem 2.1.6 ([11] Theorem 6.1)**.** *Let S and T be non-isomorphic finite simple groups. If $|S^a| = |T^b|$ for some natural numbers a and b, then $a = b$ and S and T either are $A_2(4)$ and $A_3(2)$ or are $B_n(q)$ and $C_n(q)$ for some $n \geq 3$ and some odd q.*

If a finite simple group is abelian, then all subgroups are normal, so the only proper subgroup must be the trivial subgroup $\{1\}$. It follows that abelian finite simple groups are cyclic of prime order. Our next two results concern the order of nonabelian finite simple groups. A group is *solvable* if it has a subnormal series in which all the factor groups are abelian (a subnormal series is a sequence of subgroups, each a proper normal subgroup of the next). The next theorem follows from the Feit-Thompson Odd Order Theorem, which tells us that any finite group of odd order is solvable.

Theorem 2.1.7. *A nonabelian finite simple group has even order.*

Proof. Suppose a finite simple group G is of odd order. Then by the Feit-Thompson Theorem [8], it is solvable. However, since G is also simple, the only subnormal series of G is the trivial one, $\{1\} \lhd G$. Therefore the factor group $G/\{1\}$ must be abelian. It is isomorphic to G. So G itself is abelian (and also cyclic of prime order). Therefore a nonabelian finite simple group has even order. □

We have the following corollary.

Corollary 2.1.8. *The order of a nonabelian finite simple group is divisible by* 4.

Proof. Let T be a nonabelian finite simple group. By 2.1.7, we have $|T| = 2m$ for some integer m. A group of order 2 is abelian, and so $m > 1$. The right regular representation $\widehat{T} < \mathrm{Sym}(T)$ is isomorphic to T and so is also simple. Since $\widehat{T} \cap \mathrm{Alt}(T) \trianglelefteq \widehat{T}$, we have $\widehat{T} \cap \mathrm{Alt}(T) = \widehat{T}$ (if the intersection of a permutation group with the alternating group is trivial, then the group is of order 2). Therefore $\widehat{T} \leq \mathrm{Alt}(T)$.

Now if $\widehat{g} \in \widehat{T}$, and if $\widehat{g} \neq 1_{\widehat{T}} = \widehat{1_T}$, then $\widehat{g}$ does not fix any points of T, for if $tg = t$ for some $t \in T$, then $g = 1_T$.

By the first Sylow theorem, $\widehat{T}$ has a subgroup of order 2, and hence $\widehat{T}$ has an element, $\widehat{g}$ say, of order 2. Since $\widehat{g}$ does not fix any points of T, and since $|T| = 2m$, $\widehat{g}$ must be a product of m disjoint transpositions. Then m must be even, because $\widehat{g} \in \widehat{T} \leq \mathrm{Alt}(T)$. □

The Classification of Finite Simple Groups tells us that there are three main classes of nonabelian finite simple groups. They are

Alternating groups: A_n where $n \geq 5$.

Simple groups of Lie type: comprising infinite families of groups - each family can be further classified as either classical and exceptional.

Sporadic groups: twenty six groups which do not fall into any of the families above.

Each simple group of Lie type is associated with a vector space over a finite field. There are six separate families of classical finite simple groups, and these are each parametrised by a *dimension* d and a *field order* q (of the associated vector space). Each simple group of Lie type is also associated with a Lie algebra (over the same finite field as the associated vector space), and an alternative parametrisation is by the *rank* r (of the associated algebra) and the *field order* q. Our table below is adapted from the table of classical simple groups in [12, Table 5.1.A], which shows the correspondence between two different parametrizations and different notations for the classical simple groups. This table is included here to show the relationship between rank and dimension, as we will later use Lemma 2.1.9, which concerns the rank of a classical group, together with Lemma 2.2.4 which concerns the dimension of the associated vector space. We have added a column to the table, in which we give the relationship between the rank r and the dimension d of the associated vector space.
Our next lemma follows directly from the following statement from Cameron, Neumann and Teague's paper [3, Section 4.].

> "If G_0 is a classical simple group of rank r defined over $GF(q)$ that has a proper subgroup of index n then, with finitely many exceptions, $n \geq q^r$. (See Cooperstein [6] and references quoted

Family	Lie notation and rank		Classical notation	
Linear	$A_{n-1}(q)$	$n-1$	$L_n(q)$, $\mathrm{PSL}(n,q)$	$d=r+1$
Unitary	${}^2A_{n-1}(q)$	$\lfloor n/2 \rfloor$	$U_n(q)$, $PSU(n,q)$	$\lfloor d/2 \rfloor = r$
Symplectic	$C_m(q)$	m	$PSp_{2m}(q)$, $PSp(2m,q)$	$d=2r$
Orthogonal	$B_m(q)$	m	$\Omega_{2m+1}(q)$, $P\Omega(2m+1,q)$	$d=2r+1$
Orthogonal	$D_m(q)$	m	$P\Omega^+_{2m}(q)$, $P\Omega^+(2m,q)$	$d=2r$
Orthogonal	${}^2D_m(q)$	$m-1$	$P\Omega^-_{2m}(q)$, $P\Omega^-(2m,q)$	$d=2r+2$

Table 2.1: The relationship between rank and dimension for classical simple groups

> there. In fact the only exception is $\mathrm{PSL}(2,9)$ acting as a group of degree 6)."

Lemma 2.1.9. *Let n be a positive integer such that $n \neq 6$. Let $X_r(q)$ be a classical simple group of Lie rank r. If there is a transitive (faithful) action of $X_r(q)$ of degree n, then $n \geq q^r$.*

2.2 Combinatorics

This section contains mostly unrelated results which are of a combinatorial nature.

Lemma 2.2.1. *Let n be an even positive integer. If $n \equiv 0 \pmod 4$ then*

$$\binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{n/2-1} = 2^{n-2}.$$

If $n \equiv 2 \pmod 4$, then

$$\binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{n/2-2} + \frac{1}{2}\binom{n}{n/2} = 2^{n-2}.$$

Proof. For any positive integer n, by the binomial theorem we have

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}.$$

Let n be an even positive integer. Then there are an odd number of terms in this sum, and since $\binom{n}{k} = \binom{n}{n-k}$ for $0 \leq k \leq n$, we have

$$2^{n-1} = \binom{n}{0} + \binom{n}{1} + \ldots + \frac{1}{2}\binom{n}{n/2}.$$

Let $\mathcal{P}$ be the set of partitions of $\Omega = \{1, \ldots, n\}$ into two parts. Then each element of $\mathcal{P}$ is of the form $\{\Delta, \Omega \backslash \Delta\}$ for some $\Delta \subset \Omega$ such that $0 \leq |\Delta| \leq n/2$, and $|\mathcal{P}| = 2^{n-1}$. Now let $\mathcal{E}$ be the set of partitions of $\Omega = \{1, \ldots, n\}$ into two parts of even order (this includes the partition $\{\emptyset, \Omega\}$), and let $\mathcal{O}$ be the set of partitions of Ω into two subsets of odd order. Thus we have $\mathcal{P} = \mathcal{E} \cup \mathcal{O}$. There is a bijection $\beta : \mathcal{E} \to \mathcal{O}$ defined by

$$\{\Delta, \Omega \setminus \Delta\} \mapsto \{\Delta \setminus 1, (\Omega \setminus \Delta) \cup 1\} \text{ if } 1 \in \Delta,$$
$$\{\Delta, \Omega \setminus \Delta\} \mapsto \{\Delta \cup 1, (\Omega \setminus \Delta) \setminus 1\} \text{ if } 1 \in \Omega \setminus \Delta.$$

Therefore $|\mathcal{E}| = |\mathcal{O}| = |\mathcal{P}|/2 = 2^{n-2}$.

If $n \equiv 0 \pmod 4$ then $n/2 - 1$ is odd, and so

$$|\mathcal{O}| = \binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{n/2-1},$$

and our result follows.

If $n \equiv 2 \pmod 4$, then $n/2$ is odd, and so

$$|\mathcal{O}| = \binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{n/2-2} + \frac{1}{2}\binom{n}{n/2},$$

and again our result follows.

□

The analysis of Stirling's series for the Gamma-function in Whittaker and Watson's book [19] allows us to obtain the following bounds on $r!$. (The Gamma-function is the indefinite integral $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}dt$.)

Lemma 2.2.2. *Let r be a positive integer. Then*

$$\left(\frac{r}{e}\right)^r \sqrt{re} < r! < \left(\frac{r}{e}\right)^r \sqrt{r}e^2,$$

or stated alternatively,

$$\exp\left[r \ln r - r + \tfrac{1}{2}\ln r + \tfrac{1}{2}\right] < r! < \exp\left[r \ln r - r + \tfrac{1}{2}\ln r + 2\right].$$

Proof. From [19, Section 12.12] we have that if z is a positive integer, then $\Gamma(1) = 1$ and $\Gamma(z) = (z-1)!$ so

$$z! = \Gamma(z+1) = z\Gamma(z).$$

Furthermore, from [19, Section 12.33] we have that if $x > 1$ then

$$\Gamma(x) = x^{x-\frac{1}{2}} e^{-x} (2\pi)^{\frac{1}{2}} e^{\theta/12x},$$

where $0 < \theta < 1$. If $x > 0$ then $0 < \theta/12x < 1/12$, and so $1 < e^{\theta/12x} < e^{1/12}$. Combining this with the fact that $e^{\frac{1}{2}} < (2\pi)^{\frac{1}{2}} < e$, we have that if $x > 1$ then $e^{\frac{1}{2}} < (2\pi)^{\frac{1}{2}} e^{\theta/12x} < e^{1+1/12} < e^2$. So if $x > 1$ we have

$$x^{x-\frac{1}{2}} e^{-x} e^{\frac{1}{2}} < \Gamma(x) < x^{x-\frac{1}{2}} e^{-x} e^2.$$

Therefore for any positive integer r,

$$r^{r+\frac{1}{2}} e^{-r} e^{\frac{1}{2}} < r! < r^{r+\frac{1}{2}} e^{-r} e^2.$$

□

We use this upper bound for a factorial in the next lemma.

Lemma 2.2.3. *Let n be a positive integer such that $n \geq 146$, and let k be a divisor of n such that $5 \leq k \leq \frac{n}{2}$. Then*

$$|S_{n/k} \wr S_k| \leq e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}}.$$

Proof. We apply Lemma 2.2.2.

$$\begin{aligned}
|S_{n/k} \wr S_k| &= (n/k)!^k\, k! \\
&< \exp\left[(\tfrac{n}{k} \ln \tfrac{n}{k} - \tfrac{n}{k} + \tfrac{1}{2} \ln \tfrac{n}{k} + 2)k + (k \ln k - k + \tfrac{1}{2} \ln k + 2)\right] \\
&= \exp[(n \ln n - n \ln k - n + \tfrac{k}{2} \ln n - \tfrac{k}{2} \ln k + 2k) \\
&\qquad + (k \ln k - k + \tfrac{1}{2} \ln k + 2)] \\
&= \exp\left[(n \ln n - n + 2) - n \ln k + (\tfrac{k}{2} + \tfrac{1}{2}) \ln k + (\tfrac{1}{2} \ln n + 1)k\right].
\end{aligned}$$

We examine how the exponent varies for a fixed value of n. Let n be fixed and define a function $f(x)$ on the range $[5, n/2] = \{x \in \mathbb{R} : 5 \leq x \leq n/2\}$.

$$f(x) = \tfrac{x}{2}\ln x + (\tfrac{1}{2}\ln n + 1)x + (\tfrac{1}{2} - n)\ln x + (n\ln n - n + 2).$$

Then

$$\begin{aligned}\frac{d}{dx}f(x) &= \tfrac{1}{2}\ln x + \tfrac{1}{2} + (\tfrac{1}{2}\ln n + 1) + \tfrac{1}{x}(\tfrac{1}{2} - n)\\ &= \tfrac{1}{2}\ln x + (\tfrac{1}{2}\ln n + \tfrac{3}{2}) + \tfrac{1}{x}(\tfrac{1}{2} - n),\end{aligned}$$

and

$$\begin{aligned}\frac{d^2}{dx^2}f(x) =& \tfrac{1}{2x} - \tfrac{1}{x^2}(\tfrac{1}{2} - n)\\ =& \tfrac{1}{2x^2}(2n + x - 1).\end{aligned}$$

All values of $f(x)$ are finite and the second derivative is positive (on the defined range), so if $f(x)$ does have a turning point (within this range), it must be a minimum. Now we show as long as $n \geq 146$ we have $f(5) > f(n/2)$, and then it follows that $f(5) > f(x)$ for all $x \in [5, n/2]$.

$$\begin{aligned}&f(5) - f(n/2)\\ &= [(\tfrac{5}{2} + \tfrac{1}{2} - n)\ln 5 + (\tfrac{1}{2}\ln n + 1)5] - [(\tfrac{n}{4} + \tfrac{1}{2} - n)\ln\tfrac{n}{2} + (\tfrac{1}{2}\ln n + 1)\tfrac{n}{2}]\\ &= \tfrac{1}{2}n\ln n - (\tfrac{1}{2} + \ln 5 + \tfrac{3}{4}\ln 2)n + 2\ln n + (5 + 3\ln 5 + \tfrac{1}{2}\ln 2).\end{aligned}$$

Let $g(y) = f(5) - f(y/2)$ for $y \in \mathbb{R},\ y \geq 1$. Then

$$\begin{aligned}g(y) &= \tfrac{1}{2}y\ln y - (\tfrac{1}{2} + \ln 5 + \frac{3}{4}\ln 2)y + 2\ln y + (5 + 3\ln 5 + \frac{1}{2}\ln 2),\\ \text{and } \frac{d}{dy}g(y) &= \tfrac{1}{2}\ln y + \tfrac{1}{2} - (\tfrac{1}{2} + \ln 5 + \tfrac{3}{4}\ln 2) + \tfrac{2}{y}\\ &= \tfrac{1}{2}\ln y - (\ln 5 + \tfrac{3}{4}\ln 2) + \tfrac{2}{y}.\end{aligned}$$

The first derivative is positive when $\frac{1}{2}\ln y - \big(\ln 5 + \frac{3}{4}\ln 2\big) + \frac{2}{y} \geq 0$, so is certainly positive when $y \geq e^{2(\ln 5 + \frac{3}{4}\ln 2)} = 70.7$ (to 1 decimal place) and furthermore $g(146) > 0$. It follows that $g(y) > 0$ for all $y \geq 146$, and so if

$n \geq 146$, we have $f(5) > f(n/2)$. Then since $|S_{n/k} \wr S_k| < \exp[f(k)]$, we have

$$|S_{n/k} \wr S_k| \leq \exp[f(5)] = e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}}.$$

□

We give two further useful upper bounds.

Lemma 2.2.4. *Let k and d be integers such that $1 \leq k \leq d-1$. Let V_q^d be a vector space of dimension d over $\mathbb{F}_q$, and let $L_k(V_q^d)$ be the set of k dimensional subspaces of V_q^d. Then*

$$|L_k(V_q^d)| = \frac{(q^d-1)(q^{d-1}-1)\dots(q^{d-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} \leq q^{(d+1)^2/4}.$$

Proof. The number of sets of k distinct linearly independent vectors in V_q^d (that is, the number of possible bases for a k dimensional subspace) is $(q^d-1)(q^d-q)\dots(q^d-q^{k-1})$, and the number of these sets which span the same k dimensional subspace (which is equal to the number of bases for a k dimensional vector space over $\mathbb{F}_q$) is $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$, so we have

$$\begin{aligned}|L_k(V_q^d)| &= \frac{(q^d-1)(q^d-q)\dots(q^d-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} \\ &= \frac{(q^d-1)(q^{d-1}-1)\dots(q^{d-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.\end{aligned}$$

Now for $0 \leq i \leq k-1$, we have

$$\frac{q^{d-i}-1}{q^{k-i}-1} < \frac{q^{d-i}}{q^{k-i}-1} < \frac{q^{d-i}}{q^{k-i-1}} = q^{d-k+1},$$

so $|L_k(V_q^d)| < (q^{d-k+1})^k = q^{k(d-k+1)}$. We analyse the exponent for a fixed value of d. Let $f(k) = k(d-k+1)$, then we have $f'(k) = d-2k+1$, and $f''(k) = -2$. Therefore $f(k)$ has a maximum value at $k = (d+1)/2$ and this maximum is $f((d+1)/2) = (d+1)^2/4$. □

Lemma 2.2.5. *A group of order k has at most $k^{\log_2 k}$ subgroups, and at most $k^{\log_2 k - \log_2 n}$ index n subgroups.*

Proof. Let G be a group of order k, and let $H < G$. Let $\{g_1, \ldots, g_m\}$ be a minimal set of generators for H, and for each $1 \leq i \leq m$, let $H_i = \langle g_1, \ldots, g_i \rangle$. Let $H_{m+1} = G$ and $H_0 = 1_G$. Then for each $1 \leq i \leq m+1$, we have $|H_i|/|H_{i-1}| \geq 2$, so

$$k = |G| = \frac{|H_{m+1}|}{|H_m|}\frac{|H_m|}{|H_{m-1}|}\cdots\frac{|H_1|}{|H_0|} \geq 2^{m+1} \geq 2^m,$$

and it follows that $m \leq \log_2 k$. Therefore each proper subgroup of G is generated by at most $\log_2 k$ of the k elements of G, so there are certainly at most $k^{\log_2 k}$ possible proper subgroups.

If the index of H in G is n, then we have

$$k = |G| = \frac{|H_{m+1}|}{|H_m|}\frac{|H_m|}{|H_{m-1}|}\cdots\frac{|H_1|}{|H_0|} \geq n2^m,$$

and it follows that $m \leq \log_2 k - \log_2 n$. Therefore each index n subgroup of G is generated by at most $\log_2 k - \log_2 n$ of the k elements of G, so there are certainly at most $k^{\log_2 k - \log_2 n}$ possible index n subgroups. □

Chapter 3

Constructive proofs for S_n

In this chapter we give constructive proofs for our results concerning $\mu(S_n)$ where n is odd and $n \leq 19$. This proves Theorem 1.1.1 part 1 for $n \leq 19$ and part 2.

3.1 Introduction

We give the theory discussed in our introductory chapter in a lemma. Recall that we defined a bi-cycle to be a permutation $g \in S_n$ which has precisely two orbits on $\Omega = \{1, \ldots, n\}$ (one of these orbits may be trivial of length 1).

Lemma 3.1.1. *Let n be an odd integer. Let $\mathcal{L}$ be the set containing A_n and the intransitive maximal subgroups of S_n. Then $\mathcal{L}$ is a covering for S_n of order 2^{n-1}. If $\mu(S_n) = 2^{n-1}$, then a maximal pairwise generating set for S_n consists of one n-cycle and $2^{n-1} - 1$ bi-cycles, each from a different subgroup in $\mathcal{L}$.*

The covering $\mathcal{L}$ is a good starting point to find a pairwise generating set for S_n, for if a set X consists of one n-cycle and $2^{n-1} - 1$ bi-cycles, each from a different subgroup in $\mathcal{L}$, then certainly each subgroup in $\mathcal{L}$ contains exactly one element of X. However, if X is a pairwise generating set, then no other maximal subgroup of S_n (not in $\mathcal{L}$) can contain more than one element of X either. For $n \in \{5, 7, 11, 13, 17, 19\}$, S_n has only one further conjugacy class of maximal subgroups, the affine subgroups, and S_3 has no maximal subgroups other than those in $\mathcal{L}$. This makes it quite straightforward to use a constructive proof. (Note that we have $\mu(S_1) = 2^{1-1} = 1$, since the set $\{e\}$ is (trivially) a pairwise generating set of order 2^{1-1} for $S_1 = \{e\}$.)

3.2 $n = 3$

The group S_3 of permutations of the set $\{1, 2, 3\}$ has the following elements,

$$S_3 = \{e, (12), (23), (13), (123), (132)\},$$

and the four non-trivial proper subgroups of S_3 are

$$\{e, (12)\},\ \{e, (23)\},\ \{e, (13)\} \text{ and } A_3 = \{e, (123), (132)\}.$$

The covering $\mathcal{L}$ for S_3 contains all of these subgroups, and there are the following two possibilities for a set containing one element from each subgroup,

$$X = \{(12), (23), (13), (123)\} \text{ or } X = \{(12), (23), (13), (132)\}.$$

Then clearly each subgroup of S_3 contains at most one element of X, so X generates S_3 pairwise. Therefore we have

$$\mu(S_3) \geq 4.$$

Since $\mu(S_3) \leq 4$ we have $\mu(S_3) = 4 = 2^{3-1}$. (We can see that this is a maximal pairwise generating set simply by inspection.)

3.3 $n = 5$

When $n = 5$, the covering $\mathcal{L}$ consists of A_5 together with the intransitive maximal subgroups $S_1 \times S_4$ and $S_2 \times S_3$. Since 5 is prime, S_5 has no imprimitive maximal subgroups. We know that S_5 has at least four conjugacy classes of maximal subgroups: one of these classes contains only A_5; two classes must contain the intransitive maximal subgroups $S_2 \times S_3$ and S_4 respectively; and one must contain the affine groups $\mathrm{AGL}(1,5)$. The following short `GAP` code tells us that S_5 has exactly four conjugacy classes of maximal subgroups.

```
gap> s:=SymmetricGroup(5); m:=MaximalSubgroupClassReps(s);;
gap>Length(m);
> 4;
```

The maximal subgroups of S_5 are therefore alternating, intransitive or affine. By Lemma 2.1.4, if $G \neq A_n$ is a maximal subgroup of S_n, then the number of copies of G in S_n is $n!/|G|$. The maximal subgroups of S_5 together with their orders and the number of copies are given in Table 3.1.

Class		Order	Number of copies
Alternating	A_5	60	1
Intransitive	$S_1 \times S_4$	24	5
Intransitive	$S_2 \times S_3$	12	10
Affine	$\mathrm{AGL}(1,5)$	20	6

Table 3.1: The maximal subgroups of S_5

The covering $\mathcal{L}$ is a minimal covering of S_5 of order $1+5+10 = 16 = 2^{5-1}$. If $\mu(S_5) = 2^{5-1}$, there is a pairwise generating set for S_5 of order 2^{5-1} and it would have to contain five 4-cycles, one from each of the copies of S_4 in S_5. We now rule this out, and then we determine how many 4-cycles a pairwise generating set can possibly contain.

Lemma 3.3.1. *A pairwise generating set for S_5 contains at most a total of three elements which are 4-cycles or 5-cycles.*

Proof. Let X generate S_5 pairwise. By Lemma 2.1.5, each 4-cycle is contained in exactly $\varphi(5-1) = 2$ copies of $\mathrm{AGL}(1,5)$. Since S_5 contains six copies of $\mathrm{AGL}(1,5)$, X contains at most three 4-cycles.

X contains at most one element of A_5, and therefore X contains at most one 5-cycle. However, any 5-cycle is also contained in one of the six copies of AGL$(1,5)$ and so if X contains a 5 cycle, it then contains at most two 4-cycles.

Therefore X contains at most a total of three 4-cycles and 5-cycles. □

Lemma 3.3.2. *There exists a pairwise generating set for S_5 which contains three 4-cycles.*

Proof. A 4-cycle is an odd permutation and so it is not contained in A_5, and a 4-cycle is not contained in $S_2 \times S_3$. Therefore it suffices to check that three 4-cycles are not contained in the same copy of S_4 or AGL$(1,5)$. Let $M_1, \ldots, M_6$ be the six copies of AGL$(1,5)$ in S_5, and let $T_1, \ldots, T_5$ be the five copies of S_4 in S_5. Then T_1 contains $3! = 6$ elements which are 4-cycles, say $g_1, g_1^{-1}, g_2, g_2^{-1}, g_3, g_3^{-1}$. By Lemma 2.1.5, each 4-cycle (and therefore its inverse) is contained in two copies of AGL$(1,5)$, and each copy of AGL$(1,5)$ contains exactly two 4-cycles from each of the five copies of S_4. Suppose that $g_1, g_1^{-1} \in M_1 \cap M_2$. Suppose $g_2, g_2^{-1} \in M_3 \cap M_4$ and $g_3, g_3^{-1} \in M_5 \cap M_6$. In this way T_1 induces a partition $\mathcal{P}_1$, of the set of copies of AGL$(1,5)$, that is $\mathcal{P}_1 = \{\{M_1, M_2\}, \{M_3, M_4\}, \{M_5, M_6\}\}$. Now for each distinct pair M_j, M_k of copies of AGL$(1,5)$ we have 4 divides $|M_j \cap M_k|$, and $|M_j \cap M_k|$ divides $|\text{AGL}(1,5)| = 20$, so $|M_j \cap M_k| = 4$. Each T_i induces a similar partition $\mathcal{P}_i$, but because $|M_j \cap M_k| = 4$, no two parts from these partitions are the same. Suppose without loss of generality that

$$\mathcal{P}_1 = \{\{M_1, M_2\}, \{M_3, M_4\}, \{M_5, M_6\}\},$$
$$\mathcal{P}_2 = \{\{M_1, M_3\}, \{M_2, M_5\}, \{M_4, M_6\}\},$$
$$\mathcal{P}_3 = \{\{M_1, M_4\}, \{M_2, M_6\}, \{M_3, M_5\}\},$$
$$\mathcal{P}_4 = \{\{M_1, M_5\}, \{M_2, M_4\}, \{M_3, M_6\}\},$$
$$\mathcal{P}_5 = \{\{M_1, M_6\}, \{M_2, M_3\}, \{M_4, M_5\}\}.$$

Then we can pick three 4-cycles, h_1, h_2 and h_3 such that $h_1 \in T_1 \cap M_1 \cap M_2$, $h_2 \in T_2 \cap M_4 \cap M_6$ and $h_3 \in T_3 \cap M_3 \cap M_5$. Therefore there are three 4-cycles in

S_5, no two of which are in the same maximal subgroup. Therefore a pairwise generating set can contain three 4-cycles. □

Note that the following three 4-cycles generate S_5 pairwise, and in fact this proves the previous lemma:

$$(2354),\ (1354),\ (1324).$$

A theoretical proof is included above to introduce the reader to the concept of the induced partition of the conjugacy class of subgroups S_{n-1} which will be used again in the proof of Lemma 3.4.1.

We have determined that a maximal pairwise generating set contains at most three 4-cycles. We will eventually give a construction of a maximal pairwise generating set which does have three 4-cycles, but it could equally have two 4-cycles and a 5-cycle. In Table 3.2 we recall the possible cycle structures for elements of S_5, which we will use in the proof of our next lemma (we have omitted cycles of length 1).

Cycle structure	Example	Number
-	e	1
2	(12)	10
2,2	(12)(34)	15
3	(123)	20
2,3	(12)(345)	20
4	(1234)	30
5	(12345)	24
		120

Table 3.2: The cycle structures of the elements of S_5

Lemma 3.3.3. *We have* $\mu(S_5) \leq 13$.

Proof. Let X generate S_5 pairwise. Elements of X with different cycle structures are considered in turn.

First suppose that X contains a 2-cycle. It then can not contain a (2,2)-cycle because any combination of a 2-cycle and a (2,2)-cycle is contained in some copy of $S_2 \times S_3$ or S_4. It also can not contain a 3-cycle because any combination of a 2-cycle and a 3-cycle is contained in either some copy of $S_2 \times S_3$ (if they are disjoint) or some copy of S_4 (if they are not disjoint). Furthermore, any 2-cycle is contained in four copies of $S_2 \times S_3$, and therefore X contains at most six (2,3)-cycles, which come from the remaining six copies of $S_2 \times S_3$. By Lemma 3.3.1, X contains at most a total of three 4-cycles and 5-cycles. All cycle structures have now been considered and therefore if X contains a 2-cycle, $|X| \leq 10$.

Suppose that X does not contains a 2-cycle, but does contain a (2,2)-cycle. It contains at most one (2,2)-cycle (since all (2,2)-cycles are contained in A_5), and no 3-cycles (again because of A_5). A (2,2)-cycle is contained in exactly two copies of $S_2 \times S_3$, and therefore X contains at most eight (2,3)-cycles, which come from the remaining copies of $S_2 \times S_3$. By Lemma 3.3.1, X contains at most a total of three 4-cycles and 5-cycles. All cycle structures have now been considered and therefore if X contains a (2,2)-cycle, $|X| \leq 12$.

Suppose that X does not contain a 2-cycle or a (2,2)-cycle. It contains at most one 3-cycle (since all 3-cycles are contained in A_5). A 3-cycle is contained in exactly one copy of $S_2 \times S_3$, and therefore X contains at most nine (2,3)-cycles, which come from the remaining copies of $S_2 \times S_3$. By Lemma 3.3.1, X contains at most a total of three 4-cycles and 5-cycles. All cycle structures have now been considered and therefore if X contains a 3-cycle, $|X| \leq 13$.

Finally, suppose that X does not contain a 2-cycle, a (2,2)-cycle or a 3-cycle. Since there are ten copies of $S_2 \times S_3$, X contains at most ten (2,3)-cycles. Also, by Lemma 3.3.1, X contains at most three 4-cycles and 5-cycles, and therefore again $|X| \leq 13$. □

Lemma 3.3.4. *We have* $\mu(S_5) = 13$.

Proof. Let X contain the following 13 elements:

Ten (2,3)-cycles - each one from a different copy of $S_2 \times S_3$;

Three 4-cycles - from different copies of S_4, such that no two are in the same copy of $\mathrm{AGL}(1,5)$ (this is possible by Lemma 3.3.2).

Certainly each copy of $S_2 \times S_3$ contains exactly one (2,3)-cycle from X, and clearly no 4-cycles. Three copies of S_4 contain a 4-cycle from X, and two do not contain an element of X. Each copy of $\mathrm{AGL}(1,5)$ contains one 4-cycle from X. Since all elements of $\mathrm{AGL}(1,5)$ are in cyclic subgroups of order 5 or 4, any copy of $\mathrm{AGL}(1,5)$ does not contain any (2,3)-cycles. A_5 does not contain any elements from X, since X contains only odd permutations.

Therefore each maximal subgroup contains at most one element from X, so X generates S_5 pairwise, and $\mu(S_5) \geq 13$. Then by Lemma 3.3.3, our result follows. □

3.4 $n \in \{7, 11, 13, 17, 19\}$

For all odd values of n, S_n has $(n-1)/2$ conjugacy classes of intransitive maximal subgroups. If n is prime, then S_n does not contain any imprimitive maximal subgroups, but it does have at least two conjugacy classes of primitive maximal subgroups, one which contains only A_n, and one which contains the affine groups $\mathrm{AGL}(1,p)$. Therefore we know that if $n \in \{7, 11, 13, 17, 19\}$, then S_n has at least $(n-1)/2 + 2$ conjugacy classes of maximal subgroups. The following short `GAP` code tells us that there are no more.

```
gap>for n in [7,11,13,17,19] do
>       s:=SymmetricGroup(n);
>       m:=MaximalSubgroupClassReps(s);
>       l:=Length(m)-(n-1)/2-2;
>       Print(l); od;
```

> 0 0 0 0 0

Therefore as in the case $n = 5$, for these values of n the maximal subgroups of S_n are alternating, intransitive and affine.

As discussed in the proof of Lemma 2.1.5, all the non-trivial elements of an affine maximal subgroup of S_n where n is prime are contained in cyclic subgroups of order n or $n-1$. Therefore the only elements of affine maximal subgroups which are bi-cycles are $(n-1)$-cycles.

A pairwise generating set of order 2^{n-1} for these values of n must contain n elements which are $(n-1)$-cycles, such that no pair are in the same affine maximal subgroup, and no two are in the same copy of S_{n-1} in S_n. (Recall that this was not possible for $n = 5$).

Lemma 3.4.1. *Let p be prime such that $p \geq 7$. There exists a subset of S_p of order $p+1$, which contains p elements which are $(p-1)$-cycles and one p-cycle, such that the following conditions hold.*

No two are in the same copy of $\mathrm{AGL}(1,p)$ *in S_p.*

No two are in the same copy of S_{p-1} in S_p.

Proof. By Lemma 2.1.5, a fixed $(p-1)$-cycle in S_p is contained in $\varphi(p-1)$ copies of $\mathrm{AGL}(1,p)$ in S_p.

Now for $i \in \{1, \ldots, p\}$ let T_i denote a copy of S_{p-1} in S_p. The $(p-1)$-cycles in T_i can be partitioned such that each part contains the $\varphi(p-1)$ elements which are powers of the same $(p-1)$-cycle. Let $\mathcal{P}_i$ be the corresponding partition of the set of affine maximal subgroups, where each part contains the $\varphi(p-1)$ copies of $\mathrm{AGL}(1,p)$ which contain the same $\varphi(p-1)$ elements which are $(p-1)$-cycles in T_i. Thus each $\mathcal{P}_i$ has $(p-2)!/\varphi(p-1)$ parts, and each part corresponds to $\varphi(p-1)$ elements which are $(p-1)$-cycles.

Now start with $Y = \emptyset$. Select any $(p-1)$-cycle from T_1, and add it to Y. This is contained in $\varphi(p-1)$ of the copies of $\mathrm{AGL}(1,p)$. Discard from each $\mathcal{P}_i$ all parts which contain these particular copies (i.e. discard one part from $\mathcal{P}_1$, and $\varphi(p-1)$ parts from the other $\mathcal{P}_i$). Now select a $(p-1)$-cycle from T_2 which is one of the elements which corresponds to a remaining part of $\mathcal{P}_2$, and add it to Y. Again this is contained in $\varphi(p-1)$ of the copies of $\mathrm{AGL}(1,p)$. Discard this part from $\mathcal{P}_2$, and from the other $\mathcal{P}_i$ the parts which contain these particular copies (at most $\varphi(p-1)$). Proceeding in this manner, after choosing k elements which are $(p-1)$-cycles, we have discarded at most $1+(k-1)\varphi(p-1)$ parts from each $\mathcal{P}_i$. Since initially each $\mathcal{P}_i$ has $(p-2)!/\varphi(p-1)$ parts, when Y contains p such $(p-1)$-cycles we are left with at least $(p-2)!/\varphi(p-1)-(1+(p-1)\varphi(p-1))$. Together these contain $(p-2)!-(1+(p-1)\varphi(p-1)^2)$ copies of $\mathrm{AGL}(1,p)$ which do not contain an element of Y.

Now $(p-2)!-(1+(p-1)\varphi(p-1)^2)>1$ for $p\geq 7$. Therefore we have many copies of $\mathrm{AGL}(1,p)$ left from which to select any single p-cycle, and add it to Y whilst preserving the given conditions. □

Note that the final inequality in this proof does not hold for $n=p=5$, that is $3!-(1+4\varphi(4)^2)<0$.

Lemma 3.4.2. *If $n\in\{7,11,13,17,19\}$ then $\mu(S_n)=2^{n-1}$.*

Proof. Let n be prime, $n\geq 7$. Let Y be a subset of S_n, which contains n elements which are $(n-1)$-cycles and one n-cycle, such that the following conditions hold.

No two are in the same copy of $\mathrm{AGL}(1,n)$ in S_n.

No two are in the same copy of S_{n-1} in S_n.

Such a set exists by Lemma 3.4.1. Let Z be a subset of S_n which contains $\binom{n}{r}$ elements which are $(r,n-r)$-cycles for each $2\leq r<n/2$, such that no two are in the same intransitive maximal subgroup of S_n. This is certainly always

possible since for each $2 \leq r < n/2$, there are $\binom{n}{r}$ partitions of the set Ω into precisely two subsets. Let $X = Y \cup Z$, so $|X| = 2^{n-1}$.

Then A_n, the intransitive maximal subgroups and the affine maximal subgroups each contain only one element of X. If $n \in \{7, 11, 13, 17, 19\}$ then there are no further maximal subgroups of S_n, so X generates S_n pairwise, and we have $\mu(S_n) \geq 2^{n-1}$. $\square$

In fact we will prove later that for any prime n which is not of the form $(q^d-1)/(q-1)$, the only maximal subgroups of S_n are alternating, intransitive or affine, and so this proof holds for values of n that satisfy this condition. However, all such values of n (except for those included in this section) will be covered later by our probabilistic proof.

3.5 n=9

We know that S_9 has at least seven conjugacy classes of maximal subgroups: four conjugacy classes of intransitive maximal subgroups; one conjugacy class of imprimitive maximal subgroups $S_3 \wr 3_3$; a conjugacy class of primitive maximal subgroups which contains A_9; and a conjugacy class of affine maximal subgroups $\mathrm{AGL}(2,3)$. The following `GAP` code tells us that S_9 has exactly seven conjugacy classes of maximal subgroups, so there are no more.

```
gap> s:=SymmetricGroup(9); m:=MaximalSubgroupClassReps(s);;
gap> Length(m);
> 7;
```

We give the maximal subgroups in Table 3.3.

If $\mu(S_9) = 2^{9-1}$, then by Lemma 3.1.1, there is a subset of S_9 containing a 9-cycle, and $2^{9-1} - 1$ bi-cycles which generates S_9 pairwise. In particular such a set would contain 84 elements which are $(3,6)$-cycles - exactly one from each of the $\binom{9}{3} = 84$ intransitive maximal subgroups $S_3 \times S_6$ of S_9. However, we now show that the size of the conjugacy class of imprimitive maximal subgroups

Class		Order	Number of copies
Alternating	A_9	$9!/2$	1
Intransitive	$S_1 \times S_8$	8!	9
Intransitive	$S_2 \times S_7$	2!7!	36
Intransitive	$S_3 \times S_6$	3!6!	84
Intransitive	$S_4 \times S_5$	4!5!	126
Imprimitive	$S_3 \wr S_3$	1296	280
Affine	$\mathrm{AGL}(2,3)$	432	840

Table 3.3: The maximal subgroups of S_9

$S_3 \wr S_3$ prevents a pairwise generating set from containing more than 70 elements which are $(3,6)$-cycles. In the proof of the next lemma we use the fact that there is a one-one correspondence between imprimitive maximal subgroups of S_9, and partitions of $\{1,\ldots,9\}$ into three subsets of order three, that is, the parts of the partition are the blocks for such a subgroup. This concept will be explored further in our chapter on imprimitive maximal subgroups of S_n, Chapter 6.

Lemma 3.5.1. *A fixed $(3,6)$-cycle in S_9 is contained in four distinct imprimitive maximal subgroups of S_9.*

Proof. Let $\mathcal{W}$ be the conjugacy class of imprimitive maximal subgroups $S_3 \wr S_3$ of S_9. We show that the $(3,6)$-cycle $g = (123)(456789)$ is contained in four distinct subgroups from $\mathcal{W}$.

Let $g \in H$ where $H \in \mathcal{W}$. Then there are three blocks for H and the set of blocks is a partition of $\{1,\ldots,9\}$ into three subsets of order 3. First suppose that 1 and 2 are in the same block, B_1 say. Then $B_1^g = B_1$, and it follows that $B_1^{g^i} = B_1$ for all positive integers i, so $3 \in B_1$ and $B_1 = \{1,2,3\}$. Let B_2 be the block containing 4, so $5 \notin B_2$ otherwise by a similar argument we would have $4,5,6,7,8,9 \in B_2$. It is easy to see that the blocks of H must be

$$\left\{\begin{array}{c}1\\2\\3\end{array}\right\},\left\{\begin{array}{c}4\\6\\8\end{array}\right\},\left\{\begin{array}{c}5\\7\\9\end{array}\right\}.$$

(Although the blocks are written vertically this is just for ease of display, each block is simply a set, and the relative heights of the elements is irrelevant.)

On the the other hand, if 1 and 2 are in different blocks, it is easy to see that there are the following three possibilities for the blocks of H

$$\left\{\begin{array}{c}7\\4\\1\end{array}\right\},\left\{\begin{array}{c}8\\5\\2\end{array}\right\},\left\{\begin{array}{c}9\\6\\3\end{array}\right\} \text{ or } \left\{\begin{array}{c}9\\6\\1\end{array}\right\},\left\{\begin{array}{c}7\\4\\2\end{array}\right\},\left\{\begin{array}{c}8\\5\\3\end{array}\right\} \text{ or } \left\{\begin{array}{c}8\\5\\1\end{array}\right\},\left\{\begin{array}{c}9\\6\\2\end{array}\right\},\left\{\begin{array}{c}7\\4\\3\end{array}\right\}.$$

Therefore there are four possibilities for the blocks for H, and so four possibilities for H.

Since all $(3,6)$-cycles are conjugate in S_9, this result holds for all $(3,6)$-cycles in S_9. □

Lemma 3.5.2. *We have* $\mu(S_9) < 2^{9-1}$

Proof. The imprimitive maximal subgroup $S_3 \wr S_3$ is a maximal subgroup of S_9, so by Lemma 6.3.2 there are $|S_9|/|S_3 \wr S_3| = 9!/(3!^3 3!) = 280$ copies of $S_3 \wr S_3$ in S_9.

By Lemma 3.5.1, a fixed $(3,6)$-cycle in S_9 is contained in four distinct copies of $S_3 \wr S_3$ in S_9, and we know that in a pairwise generating set no two elements can be contained the same maximal subgroup. Therefore a pairwise generating set for S_9 contains at most $280/4 = 70$ elements which are $(3,6)$-cycles. However we remarked earlier that if $\mu(S_9) \geq 2^{9-1}$, then a pairwise generating set exists which contains 84 elements which are $(3,6)$-cycles. Therefore $\mu(S_9) < 2^{9-1}$. □

Our next proof uses a list of permutations which generates S_9 pairwise. This list was obtained using a `GAP` program to choose $(3,6)$-cycles randomly from different intransitive maximal subgroups $S_3 \times S_6$ and add this to the list, then after each selection checking that the set of elements in the list does indeed generate S_9 pairwise. Then 8-cycles from S_8 were added manually. The `GAP` program made different lists of varying sizes with each run; that used in this proof was the largest, and contains sixty four $(3,6)$-cycles.

Lemma 3.5.3. *We have* $235 \leq \mu(S_9) \leq 244$.

Proof. Let Y be the pairwise generating set for S_9 of order 73 which is listed in Appendix A and consists of the following:

9 elements which are 8-cycles,

64 elements which are $(3,6)$-cycles.

In `GAP` we define the variable `y` to be a list of the elements of Y. Then the following code returns `true`, which confirms that indeed the set Y does generate S_9 pairwise.

```
gap>x:=[y[1]];
>for g in y do tally:=[];
>   for h in x do
>      if Order(Group(g,h))=Factorial(9) then Add(tally,h); fi;
>   od;
>   if tally=x then Add(x,g); fi;
>od;
gap>x=y;
>true
```

The only bi-cycles in S_9 which are contained in imprimitive maximal subgroups $S_3 \wr S_3$ are $(3,6)$-cycles and 9-cycles. The following `GAP` code returns `[[1,8],[3,6],[9]]`, which tells us that the only bi-cycles which are contained in affine maximal subgroups $\mathrm{AGL}(2,3)$ are $(1,8)$-cycles, $(3,6)$-cycles and 9-cycles.

```
gap>mscr:=MaximalSubgroupsClassReps(SymmetricGroup(9));
>m:=mscr[7]; bicycles:=[];
>for c in ConjugacyClasses(m) do
>   cl:=CycleLengths(Representative(c),[1..9]);
>   if (Length(cl)=2 or Length(cl)=1)
```

```
>                   and (AsSet(cl) in bicycles)=false then
>       Add(bicycles,AsSet(cl));
>   fi;
>od;
```

No bi-cycles are contained in A_9. Therefore we can choose $\binom{9}{2} = 36$ elements which are $(2,7)$-cycles, and $\binom{9}{4} = 126$ elements which are $(4,5)$-cycles from distinct intransitive maximal subgroups, and be sure that no pair of these elements is contained in any other maximal subgroup of S_9. Let Z be a pairwise generating set for S_9 of order $36 + 126 = 162$ which consists of the following:

$\binom{9}{2} = 36$ elements which are $(2,7)$-cycles,

$\binom{9}{4} = 126$ elements which are $(4,5)$-cycles.

Let $X = Y \cup Z$, so $|X| = 162 + 73 = 235$. No pair of elements of X is contained in a maximal subgroup of S_9, so X generates S_9 pairwise and we have $\mu(S_9) \geq 235$.

Now let X be a pairwise generating set for S_9 of order $\mu(S_9)$. An element g of S_9 which has three distinct orbits on Ω is contained in A_9 since then either all of the orbits of g are of odd length, or only one is of odd length, but in both of these cases, g is an even permutation. Let x be the number of elements of X which are either 9-cycles, or have three distinct orbits on Ω, and note that $x \leq 1$. Let y be the number of bi-cycles in X. Then by Lemma 3.5.1 we have $y \leq \binom{9}{1} + \binom{9}{2} + 70 + \binom{9}{4} = 241$. Let z be the number of elements of X which have four or more orbits on Ω. Note that such an element g is contained in at least ten different intransitive maximal subgroups, for if orbits of g are $\Delta_1, \ldots, \Delta_4$, then g is contained in the intransitive maximal subgroup which has orbits Δ and $\Omega \setminus \Delta$, where $\Delta = \Delta_i$ for any i, or $\Delta = \Delta_i \cup \Delta_j$ for any distinct pair Δ_i, Δ_j. There are $\binom{4}{1} + \binom{4}{2} = 10$ such possibilities for Δ.

Therefore $|X| = x+y+z$, and since each element in the cover $\mathcal{L}$ contains at most one element of X we have $x+y+10z \leq 256$, so $|X| \leq 256-9z$. Since we know that $|X| \geq 235$, we must have $z \leq 2$. Therefore $|X| \leq 242+2 = 244$. $\square$

We know that a pairwise generating set for S_9 can contain between sixty four and seventy $(3,6)$-cycles, and we would like to determine this precisely. However since $\binom{84}{70} > 2^{50}$, and $(2!5!)^{70} > 2^{550}$, there are more than 2^{600} sets of seventy $(3,6)$-cycles, each of which are from a different copy of $S_3 \times S_6$. This is too many to check all possible combinations.

It is possible that a faster computer programming language could be used to randomly select elements from different intransitive maximal subgroups in a similar way to our program which found a set of sixty four $(3,6)$-cycles which pairwise generate S_9. Alternatively, further study of the maximal subgroups of S_9 could lead to an exact value for $\mu(S_9)$.

3.6 n=15

Using `GAP`, we know that S_{15} does not have any primitive maximal subgroups other than A_{15}, and bi-cycles that are contained in imprimitive maximal subgroups of S_{15} are 15-cycles, $(3,12)$-cycles, $(5,10)$-cycles and $(6,9)$-cycles. It follows that

$$\mu(S_{15}) \geq \binom{15}{1} + \binom{15}{2} + \binom{15}{4} + \binom{15}{7} + \binom{15}{8} = 2^{15-1} - [\binom{15}{0} + \binom{15}{3} + \binom{15}{5} + \binom{15}{6}].$$

However, neither constructive or probabilistic methods have so far yielded a full solution to this case.

Chapter 4

Overview of proof for S_n using the probabilistic method

When n is odd and $n \geq 21$, it is cumbersome to use our constructive proofs that $\mu(S_n) = 2^{n-1}$, so we use a probabilistic method. In this chapter we present an overview of our proof using this method. This motivates Chapters 5, 6 and 7, which provide the results necessary for our actual proof of Theorem 1.1.1 part 1 for $n \geq 21$, which is given in Chapter 8.

4.1 Introduction

Let n be an odd integer such that $n \geq 21$. Recall that in Lemma 3.1.1 we proved that if $\mathcal{L}$ is the set containing A_n and the intransitive maximal subgroups of S_n, then $\mathcal{L}$ is a covering for S_n of order 2^{n-1}. Furthermore if $\mu(S_n) = 2^{n-1}$, then a maximal pairwise generating set for S_n consists of one n-cycle and $2^{n-1} - 1$ bi-cycles, each from a different subgroup in $\mathcal{L}$.

We use Blackburn's method (given first in [2]) to choose a set X which has this property. Then we study the probability that any fixed pair of distinct elements of X is contained in a proper subgroup of S_n. We prove that this probability is so low, that the probability that no pair of distinct elements of X is contained in any proper subgroup of S_n is non-zero, or equivalently, the probability that X generates S_n pairwise is non-zero. We conclude that a pairwise generating set of order 2^{n-1} exists, so $\mu(S_n) \geq 2^{n-1}$. Since $\mu(S_n) \leq \sigma(S_n) = 2^{n-1}$ (except when $n = 9$), part 1 of Theorem 1.1.1 for $n \geq 21$ follows. Different techniques are required, depending on the value of n under consideration.

4.2 Choosing a pairwise generating set

We write Ω for the set $\{1, 2, \ldots, n\}$, and let

$$I = \{\Delta \subset \Omega : |\Delta| < n/2\}.$$

Since n is odd, I contains precisely half of the subsets of Ω, so $|I| = 2^{n-1}$. For a subset $\Delta \subset \Omega$, define

$$C(\Delta) = \{g \in S_n : g \text{ is a } (|\Delta|, n - |\Delta|)\text{-cycle such that } \Delta g = \Delta\}.$$

If $\Delta \neq \emptyset$, the elements of $C(\Delta)$ are all of the bi-cycles from S_n which have orbits Δ and $\Omega \setminus \Delta$, that is, all of the bi-cycles from a single intransitive maximal subgroup. The elements of $C(\emptyset)$ are all of the n-cycles from S_n. Now for each $\Delta \in I$, choose $g_\Delta \in C(\Delta)$ uniformly and independently at random. Then define

$$X = \{g_\Delta : \Delta \in I\}.$$

Since $|X| = |I|$, we have $|X| = 2^{n-1}$.

Certainly X contains precisely one element from each subgroup in our covering of S_n. However, it is possible that a distinct pair of elements of X is contained in some subgroup not in the covering, which would mean that X does not generate S_n pairwise. The probability of this is low.

We aim to show that the probability is suffiently low that we can conclude that a set X chosen in this way exists, which does indeed generate S_n pairwise. The Lovász Local lemma provides us with the tool to reach this conclusion.

4.3 The Lovász Local lemma

Lemma 4.3.1 (Lovász Local lemma (see [1])). *Let $\Gamma = (V, E)$ be a finite graph with minimum valency d. Suppose that we associate an event E_v to every vertex $v \in V$, and suppose that E_v is independent of any subset of the events $\{E_u : u \nsim v\}$. Let p be such that $Pr(E_v) < p$ for all v. Then $Pr(\bigcap_{v \in V} \overline{E_v}) > 0$ whenever $ep(d+1) < 1$ (where e is the constant such that $\ln e = 1$).*

We define a graph $\Gamma = (V, E)$ as follows. The vertices of Γ are the two element subsets of I. For example for each pair $\Delta_1, \Delta_2 \in I$ such that $\Delta_1 \neq \Delta_2$, we have a vertex $\{\Delta_1, \Delta_2\}$. A pair v, v' of vertices are joined by an edge precisely when $v \cap v' \neq \emptyset$. Therefore

$$|V| = \binom{|I|}{2} = 2^{n-1}(2^{n-1} - 1)/2 = 2^{n-2}(2^{n-1} - 1),$$

and each vertex has valency d, where

$$d = 2(|I| - 2) = 2(2^{n-1} - 2) = 2^n - 4.$$

Now we fix a distinct pair Δ_1, Δ_2 of elements of I, and thus fix the corresponding vertex $\{\Delta_1, \Delta_2\}$ of the graph Γ. We write $E_{\{\Delta_1, \Delta_2\}}$ for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of S_n. This is the same as the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a proper subgroup of S_n, which is the same as the event that $\langle g_{\Delta_1}, g_{\Delta_2} \rangle$ is a proper subgroup of S_n, and the same as the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ does not generate S_n. It is clear that $E_{\{\Delta_1, \Delta_2\}}$ is independent of any subset of the events E_u, where $u \in V$ is not adjacent to $\{\Delta_1, \Delta_2\}$.

We define $p = 1/e2^n$ so we have $ep(d+1) < 1$ and, we will prove that

$$Pr(E_{\{\Delta_1, \Delta_2\}}) < p,$$

or if it is more convenient we will prove directly that

$$e(d+1)\, Pr(E_{\{\Delta_1, \Delta_2\}}) < 1.$$

Since $\{\Delta_1, \Delta_2\}$ is an arbitrary vertex of the our graph Γ, the conditions of the Lovász Local lemma are satisfied, and we may conclude that $Pr(\bigcap_{v \in V} \overline{E}_v) > 0$. Obviously $\bigcap_{v \in V} \overline{E}_v$ is precisely the event that X generates S_n pairwise. So can conclude that the probability that X generates S_n pairwise is non-zero. Therefore a pairwise generating set of order 2^{n-1} exists, so $\mu(S_n) \geq 2^{n-1}$. Since $\mu(S_n) \leq \sigma(S_n) = 2^{n-1}$ (except when $n = 9$), part 1 of Theorem 1.1.1 for $n \geq 21$ follows.

4.4 Small, medium and large values of n

The full proof using the probabilistic method is given in Chapter 8. There are separate sections for small, medium and large values of n, as different techniques are required.

We say that values of n which greater than or equal to 225 are *large* values of n. For these values we follow closely the methods used in [2]. We differ from [2] in two respects. Where that paper uses an asymptotic bound for the probability that our pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup which is permutation isomorphic to $S_{n/3} \wr S_3$, we use a bound which is an explicit function of n. Also, where that paper uses an asymptotic bound for the number of conjugacy classes of primitive maximal subgroups of S_n, we use explicit bounds. These methods allow us to prove that if $n \geq 225$ then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$.

For $n < 225$, if we use the method above which successfully proves our result for large values of n, the upper bound for the probability that our pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup exceeds p. Therefore we need to calculate a more accurate upper bound for this probability. The system for computational discrete algebra, `GAP` (`G`roups, `A`lgorithms, `P`rogramming), provides a convenient tool for these calculations. The theory which we use in the `GAP` programs is developed in Chapter 6. For the *medium* values of n, that is where $33 \leq n \leq 223$, we apply this theory to prove that $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$.

Finally we deal with the remaining *small* values of n, that is less than 33. GAP is used again - as well as calculating probabilites as for medium values of n, this time the GAP data library provides specific detail about maximal subgroups of S_n. For these values we prove directly that $e(d+1)\,Pr(E_{\{\Delta_1,\Delta_2\}}) < 1$.

We prove results concerning probabilities in Chapter 5, concerning imprimitive maximal subgroups of S_n in Chapter 6, and concerning primitive maximal subgroups of S_n in Chapter 7.

Chapter 5

Probabilities

In this chapter we give results concerning upper bounds for some probabilities which we require for our proof using the probabilistic method, and which motivates our work in the next two chapters on imprimitive and primitive maximal subgroups of S_n.

5.1 Introduction

Let n be an integer such that $n \geq 3$, and let $\Omega = \{1, \dots, n\}$. (In our previous chapter we considered only odd values of n, but now we consider all positive integers n.) Let $\Delta_1, \Delta_2 \subset \Omega$ such that $|\Delta_1|, |\Delta_2| \leq n/2$, and $\Delta_1 \neq \Delta_2$. Now for $i \in \{1, 2\}$, define

$$C(\Delta_i) = \{g \in S_n : g \text{ is a } (|\Delta_i|, n - |\Delta_i|)\text{-cycle such that } \Delta_i g = \Delta_i\}.$$

If $\Delta_i \neq \emptyset$, the elements of $C(\Delta_i)$ are all of the bi-cycles from S_n which have orbits Δ_i and $\Omega \setminus \Delta_i$. The elements of $C(\emptyset)$ are all of the n-cycles from S_n. For $i \in \{1, 2\}$ choose $g_{\Delta_i} \in C(\Delta_i)$ uniformly and independently at random.

Lemma 5.1.1. *Let $\mathcal{H}$ be a set of subgroups of S_n. Then*

$$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ for some } H \in \mathcal{H}) \leq \sum_{H \in \mathcal{H}} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|}.$$

Proof. We have

$$\begin{aligned} Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ for some } H \in \mathcal{H}) &\leq \sum_{H\in\mathcal{H}} Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H) \\ &= \sum_{H\in\mathcal{H}} Pr(g_{\Delta_1} \in H) \times Pr(g_{\Delta_2} \in H) \\ &= \sum_{H\in\mathcal{H}} \frac{|C(\Delta_1)\cap H|}{|C(\Delta_1)|}\frac{|C(\Delta_2)\cap H|}{|C(\Delta_2)|} \end{aligned}$$

□

5.2 Some upper bounds

We apply Lemma 5.1.1 to the case where $\mathcal{H}$ is a single conjugacy class of subgroups of S_n or A_n, and then to the case where $\mathcal{H}$ is a union of conjugacy classes of subgroups of S_n or A_n. We first extend a result from [2].

Lemma 5.2.1. *Let $n \geq 3$ be an integer, and let G be a subgroup of S_n. If $g \in S_n$ is an n-cycle, then g is contained in less than n conjugates of G in S_n. If $g \in S_n$ is a bi-cycle, then g is contained in less than n^2 conjugates of G in S_n*

Proof. We count pairs (h, H) in two ways, where h is an element of S_n which is conjugate to g, and H is a subgroup of S_n containing h and which is conjugate to G. Let r be the number of such pairs.

Let g be an n-cycle. First we have $r = xy$ where x is the number of elements of S_n which are conjugate to g, and y is the number of conjugates of G in S_n which contain any fixed n-cycle - this number is the same for all n-cycles because all n-cycles are conjugate in S_n. Then $x = (n-1)!$ and y is the number for which we we want to determine an upper bound, and $r = (n-1)!y$. Second we have $r = zw$, where z is the number of n-cycles in any fixed conjugate of G in S_n (again this number is the same for all conjugates of G because all n-cycles are conjugate in S_n), and w is the number of conjugates of G. Clearly $z < |G|$, and by the orbit-stabiliser theorem, $w = |S_n : N_{S_n}(G)| \leq n!/|G|$. So

$r < n!$. Comparing these two results for r gives $(n-1)!y < n!$, so we have $y < n$.

Now let g be an $(s, n-s)$-cycle where $1 \leq s \leq n/2$. First we have $r = xy$ where x is the number of elements of S_n which are conjugate to g, and y is the number of conjugates of G in S_n which contain any fixed $(s, n-s)$-cycle - this number is the same for all n-cycles because all $(s, n-s)$-cycles are conjugate in S_n. Then if $s < n/2$ then $x = \binom{n}{s}(s-1)!(n-s-1)! = n!/s(n-s)$ and again y is the number for which we we want to determine an upper bound, so $r = y\,n!/s(n-s)$. If $s = n/2$, then $x = \frac{1}{2}\binom{n}{n/2}(n/2-1)!(n/2-1)! = 2n!/n^2$, so $r = 2y\,n!/n^2$. Second we have $r = zw$, where z is the number of $(s, n-s)$-cycles in any fixed conjugate of G in S_n, and w is the number of conjugates of G. Clearly $z < |G|$ and by the orbit-stabiliser theorem, $w = |S_n : N_{S_n}(G)| \leq n!/|G|$. So again $r < n!$. Comparing these two results for r gives $y\,n!/s(n-s) < n!$ if $s < n/2$, and $2y\,n!/n^2 < n!$. So we have $y < n^2$. $\square$

For a subgroup M of X, we write $[M]_X$ for the conjugacy class containing M, that is the set of subgroups of X which are conjugate to M by an element of X.

Lemma 5.2.2. *Let n be an integer such that $n \geq 3$, let X be S_n or A_n, and let $M < X$. Then*

$$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ for some } H \in [M]_X) \leq \frac{n^2|M|}{|C(\Delta_1)|}.$$

Proof. From Lemma 5.1.1,

$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H$ for some $H \in [M]_X)$

$$\leq \sum_{H \in [M]_X} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|}$$
$$= \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in [M]_X} |C(\Delta_1) \cap H||C(\Delta_2) \cap H|.$$

For all $H \in [M]_X$, we have $|C(\Delta_1) \cap H| \leq |H| = |M|$, so

$$\frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in [M]_X} |C(\Delta_1) \cap H||C(\Delta_2) \cap H|$$

$$\leq \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in [M]_X} |M||C(\Delta_2) \cap H|$$
$$= \frac{|M|}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in [M]_X} |C(\Delta_2) \cap H|.$$

From Lemma 5.2.1 we know that a fixed bi-cycle is contained in at most n^2 conjugates of any subgroup of X, so

$$\sum_{H \in [M]_X} |C(\Delta_2) \cap H| \leq n^2 |C(\Delta_2)|.$$

Substituting this we have

$$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ for some } H \in [M]_X) \leq \frac{|M|}{|C(\Delta_1)||C(\Delta_2)|} \times n^2 |C(\Delta_2)|$$
$$= \frac{n^2 |M|}{|C(\Delta_1)|}.$$

□

Now we apply the above to a set of conjugacy classes of subgroups. This follows directly from the above and so is stated without a proof.

Lemma 5.2.3. *Let n be an integer such that $n \geq 3$, let X be S_n or A_n, and let $\mathcal{M}$ be a set of conjugacy classes of subgroups of X. Let M be an upper bound for $|\mathcal{M}|$, and let m be an upper bound for the order of all the groups in all the conjugacy classes in $\mathcal{M}$. Then*

$$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \textit{ for some } H \in [M]_X \textit{ for some } [M]_X \in \mathcal{M})$$

$$\leq \frac{n^2 m \mathsf{M}}{|C(\Delta_1)|}.$$

This lemma motivates the work on primitive maximal subgroups in Chapter 7, where we find upper bounds for the number of conjugacy classes of particular types of primitive maximal subgroups of S_n. Our final lemma in this section provides a lower bound for $C(\Delta)$ as a function of n which we can use together with the previous two results. We use the convention that $0! = 1$.

Lemma 5.2.4. *Let n be an integer such that $n \geq 3$ and let $\Delta \subset \Omega$ such that $|\Delta| \leq n/2$. Then if n is odd we have*

$$|C(\Delta)| \geq \left(\tfrac{n-1}{2}\right)! \left(\tfrac{n-3}{2}\right)!,$$

and if n is even we have

$$|C(\Delta)| \geq \left(\tfrac{n-2}{2}\right)!^2.$$

In both cases we have

$$|C(\Delta)| \geq e^2 \left(\tfrac{n-3}{2e}\right)^{n-1}.$$

Proof. First note that $C(\emptyset) = (n-1)!$, so the first two inequalities hold for $\Delta = \emptyset$. Now suppose that $\Delta \neq \emptyset$. Then we have $|C(\Delta)| = (|\Delta| - 1)!(n - |\Delta| - 1)!$, so

$$|C(\Delta)| \geq \min_{1 \leq d < n/2} (d-1)!(n-d-1)!.$$

If d is an integer such that $1 \leq d \leq (n-1)/2$, we have $2d \leq n-1$ and so $d \leq n-d-1$, and $d/(n-d-1) \leq 1$. Therefore

$$\begin{aligned}((d+1)-1)!(n-(d+1)-1)! &= d!(n-d-2)! \\ &= (d-1)!(n-d-1)! \times d/(n-d-1) \\ &\leq (d-1)!(n-d-1)!\end{aligned}$$

Therefore if n is odd

$$\begin{aligned}\min_{1 \leq d \leq n/2} (d-1)!(n-d-1)! &= ((n-1)/2-1)!(n-(n-1)/2-1)! \\ &= \left(\tfrac{n-1}{2}\right)! \left(\tfrac{n-3}{2}\right)!,\end{aligned}$$

and if n is even

$$\begin{aligned}\min_{1\leq d\leq n/2}(d-1)!(n-d-1)! &= (n/2-1)!(n-n/2-1)!\\ &= \left(\tfrac{n-2}{2}\right)!^2.\end{aligned}$$

We now apply the consequence of Stirling's formula proved in Lemma 2.2.2, that is, $r! > \left(\frac{r}{e}\right)^r \sqrt{re}$.

$$\begin{aligned}\left(\tfrac{n-1}{2}\right)!\left(\tfrac{n-3}{2}\right)! &\geq \left(\tfrac{n-3}{2e}\right)^{\frac{n-3}{2}}\sqrt{\tfrac{(n-3)e}{2}}\left(\tfrac{n-1}{2e}\right)^{\frac{n-1}{2}}\sqrt{\tfrac{(n-1)e}{2}}\\ &= e^2\tfrac{(n-3)^{n/2-1}(n-1)^{n/2}}{(2e)^{n-1}}\\ &\geq e^2\left(\tfrac{n-3}{2e}\right)^{n-1},\end{aligned}$$

and

$$\begin{aligned}\left(\tfrac{n-2}{2}\right)!^2 &\geq \left[\left(\tfrac{n-2}{2}\right)^{\frac{n-2}{2}}\sqrt{\tfrac{(n-2)e}{2}}\right]^2\\ &= e^2\left(\tfrac{n-2}{2e}\right)^{n-1}\\ &\geq e^2\left(\tfrac{n-3}{2e}\right)^{n-1}.\end{aligned}$$

□

Chapter 6

Imprimitive maximal subgroups

In this chapter we discuss the imprimitive maximal subgroups of the symmetric group, and we give an explicit upper bound for the probability that a pair of bi-cycles selected randomly from two different intransitive maximal subgroups is contained in an imprimitive maximal subgroup $S_{n/3} \wr S_3$. We also determine an upper bound for the probability that the pair is contained in any imprimitive maximal subgroup. These bounds are needed in Chapter 8 for the proof of Theorem 1.1.1 using the probabilistic method.

6.1 Introduction

Let n be any positive integer, and let $\Delta_1, \Delta_2 \subset \Omega = \{1, \ldots, n\}$ such that $|\Delta_1|, |\Delta_2| \leq n/2$, and $\Delta_1 \neq \Delta_2$. Recall that for a subset $\Delta \subset \Omega$, we define $C(\Delta)$ to be the set of elements of S_n which have orbits Δ and $\Omega \setminus \Delta$ on Ω (so if $\Delta \neq \emptyset$ then $C(\Delta)$ is a set of bi-cycles, and $C(\emptyset)$ is the set of n-cycles in S_n). For $j \in \{1, 2\}$, let g_{Δ_j} be selected uniformly and independently at random from $C(\Delta_j)$.

In Sections 6.2 and 6.3 we give some background and preliminary results on imprimitive maximal subgroups of S_n, and bi-cycles which are contained in these subgroups. In Section 6.4 we adapt a lemma and its proof from [2]. This provides an explicit upper bound for the probability that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup $S_{n/3} \wr S_3$ of S_n. When used with

Lemmas 2.2.3 and 5.2.3 (to take into account the other imprimitive maximal subgroups), this gives an explicit upper bound for the probability that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in any imprimitive maximal subgroup of S_n. We use this bound later for large values of n. This bound however, is too high to be of use for medium and small values of n. In Section 6.5 we develop the theory which allows us to calculate a tighter, but more complicated upper bound for the probability that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in any imprimitive maximal subgroup of S_n. We use this bound later in a `GAP` program, for medium and small values of n.

6.2 The imprimitive action of a wreath product

An imprimitive action of a group is a transitive action for which there exists system of blocks. We describe an imprimitive faithful action of degree n of the wreath product $S_{n/k} \wr S_k$ where k is a non-trivial divisor of n. This action is often called the *standard* action. (There is also a primitive action of a wreath product, which is referred to as the *product* action.)

We use the definition of the wreath product of two permutation groups given in Chapter 2. That is $S_{n/k} \wr S_k$ is the semi-direct product $S_{n/k}^k :_\phi S_k$, where ϕ is the homomorphism $\phi : S_k \rightarrow \mathrm{Aut}(S_{n/k}^k)$, defined as follows. For $h \in S_k$, and $(g_1, \ldots, g_m) \in S_{n/k}^k$, let

$$\phi(h) : (g_1, \ldots, g_l) \mapsto (g_{1^{h^{-1}}}, \ldots, g_{l^{h^{-1}}}).$$

Therefore elements of $S_{n/k} \wr S_k$ are of the form $(\underline{g}, h)$ where $\underline{g} = (g_1, \ldots, g_k)$ is an element of the *base group* $S_{n/k}^k$ and y is an element of the *top group* S_k. The definition of the product of two elements $(\underline{g}, h)$ and $(\underline{x}, y)$ in a semi-direct product gives us

$$\begin{aligned}(\underline{g}, h)(\underline{x}, y) &= (\underline{g}\underline{x}^{\phi(h^{-1})}, hy)\\ &= ((g_1, \ldots, g_k)(x_{1^h}, \ldots, x_{k^h}), hy)\\ &= ((g_1 x_{1^h}, \ldots, g_k x_{k^h}), hy).\end{aligned}$$

Lemma 6.2.1. *The following rule defines an imprimitive action of* $S_{n/k} \wr S_k$ *on* $\{1, \ldots, n/k\} \times \{1, \ldots, k\}$. *For* $(i, j) \in \{1, \ldots, n/k\} \times \{1, \ldots, k\}$ *and* $(\underline{g}, h) \in S_{n/k} \wr S_k$, *where* $\underline{g} = (g_1, \ldots, g_k) \in S_{n/k}^k$ *and* $h \in S_k$, *let*

$$(i, j)^{(\underline{g}, h)} = (i^{g_j}, j^h).$$

There is exactly one block system under this action; the blocks are $\{1, \ldots, n/k\} \times \{j\}$ *for* $j \in \{1, \ldots, k\}$.

Proof. To prove that the rule given defines an action, we must show that for all $(\underline{g}, h)$ and $(\underline{x}, y)$ in $S_{n/k} \wr S_k$ and $(i, j) \in \{1, \ldots, n/k\} \times \{1 \ldots, k\}$, we have

$$[(i, j)^{(\underline{g}, h)}]^{(\underline{x}, y)} = (i, j)^{[(\underline{g}, h)(\underline{x}, y)]}.$$

Indeed, from the definitions we have that

$$\begin{aligned}[(i, j)^{(\underline{g}, h)}]^{(\underline{x}, y)} &= (i^{g_j}, j^h)^{(\underline{x}, y)}\\ &= (i^{g_j x_{j^h}}, j^{hy})\\ &= (i, j)^{[(\underline{g}, h)(\underline{x}, y)]}.\end{aligned}$$

For each $j \in \{1, \ldots, k\}$, let $B_j = \{1, \ldots, n/k\} \times \{j\}$. Then B_j is a block since

$$\begin{aligned}B_j^{(\underline{g}, h)} &= \{(i, j)^{(\underline{g}, h)} : i \in \{1, \ldots, n/k\}\}\\ &= \{(i, j^h) : i \in \{1, \ldots, n/k\}\} = B_{j^h}.\end{aligned}$$

These are the only blocks by the following argument. Let B be a block, let $(i, j), (i', j') \in B$ and let $(r, s) \in \{1, \ldots, n/k\} \times \{1 \ldots, k\}$. We will show that if $j \neq j'$, then $(r, s) \in B$. Suppose that $j \neq j'$ and $j' \neq s$. Let $\underline{g}$ be the element of $S_{n/k}^k$ with the transposition $(i\,r)$ in the jth position, and with $1_{S_{n/k}}$ elsewhere, and let $h = (j\,s)$. Then $(i', j')^{(\underline{g},h)} = (i', j') \in B$, so $(\underline{g}, h)$ fixes B and $(i, j)^{(\underline{g},h)} = (i^{g_j}, j^h) = (i^{(i\,r)}, j^{(j\,s)}) = (r, s) \in B$. Suppose that $j \neq j'$ and $j' = s$, then we may use the same argument with j and j' exchanged to show that $(r, s) \in B$. Since B is a block it is a proper subset of Ω, so we must conclude that $j = j'$.

Now we show that if $(i, j), (i', j) \in B$, then $(r, j) \in B$ for all $r \in \{1, \ldots, n/k\}$. Let $\underline{g}$ be the element of $S_{n/k}^k$ with $(i\,r)$ in the jth position, and with $1_{S_{n/k}}$ elsewhere, and let $h = 1_{S_k}$. Then $(i', j)^{(\underline{g},h)} = (i', j) \in B$, so $(\underline{g}, h)$ fixes B and $(i, j)^{(\underline{g},h)} = (i^{g_j}, j^h) = (r, j) \in B$.

Therefore any block is of the form $\{1, \ldots, n/k\} \times \{j\}$ for some $j \in \{1, \ldots, k\}$.

□

To visualise the action, we put the elements of $\{1, \ldots, n/k\} \times \{1, \ldots, k\}$ in an array with n/k rows and k columns, as shown below. We let the element (i, j) be the entry in the ith row and the jth column in an array on the left hand side, and the image of (i, j) under the action of $(\underline{g}, h)$ in the same position in an array on the right. For each j we let $B_j = \{1, \ldots, n/k\} \times \{j\}$ thus B_j is the block which consists of the n/k entries originally in the j-th column, and we write B_j at the head of the column containing this block.

$$\begin{array}{|ccc|}\hline B_1 & \cdots & B_k \\ \hline (1,1) & \cdots & (1,k) \\ \vdots & & \vdots \\ (n/k,1) & \cdots & (n/k,k) \\ \hline \end{array} \mapsto \begin{array}{|ccc|}\hline B_{1^h} & \cdots & B_{k^h} \\ \hline (1^{g_1},1^h) & \cdots & (1^{g_k},k^h) \\ \vdots & & \vdots \\ (n/k^{g_1},1^h) & \cdots & (n/k^{g_k},k^h) \\ \hline \end{array}$$

Using the techniques given on page 16 we see that $S_{n/k} \wr S_k$ acting in this way is permutation isomorphic to all the subgroups in a conjugacy class of subgroups of S_n. That is, a bijection $\psi : \{1, \ldots, n/k\} \times \{1, \ldots, k\} \to \Omega$ gives an equivalent action of $S_{n/k} \wr S_k$ on Ω, if we define

$$\omega^{(\underline{g},h)} = \psi([\psi^{-1}(\omega)]^{(\underline{g},h)}) \text{ for } \omega \in \Omega \text{ and } (\underline{g}, h) \in S_{n/k} \wr S_k.$$

Let $\sigma : S_{n/k} \wr S_k \to S_n$ be the homomorphism defined by the following rule

$$\omega^{\sigma(\underline{g},h)} = \omega^{(\underline{g},h)} \text{ for all } \omega \in \Omega.$$

Then σ is the permutation representation of this action of $S_{n/k} \wr S_k$ on Ω, and $\operatorname{Im}\sigma$ is an imprimitive subgroup of S_n, with blocks $\psi(B_1), \ldots, \psi(B_k)$.

Example 6.2.1. Let $n = 12$ and $k = 4$. The wreath product $S_3 \wr S_4$ acts imprimitively on the set $\{1,2,3\} \times \{1,2,3,4\}$. We look at the action of the element $(\underline{g}, h)$, where $\underline{g} = ((12), e, (23), (123))$ and $h = (234)$. We write the elements of $\{1,2,3\} \times \{1,2,3,4\}$ in an array on the left, and we write the image of each element under $(\underline{g}, h)$ in the corresponding position in an array on the right.

B_1	B_2	B_3	B_4		B_1	B_3	B_4	B_2
$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$		$(2,1)$	$(1,3)$	$(1,4)$	$(2,2)$
$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	$\mapsto$	$(1,1)$	$(2,3)$	$(3,4)$	$(3,2)$
$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$		$(3,1)$	$(3,3)$	$(2,4)$	$(1,2)$

Now let $\psi : \{1,2,3\} \times \{1,2,3,4\} \to \{1,\ldots,12\}$ be the bijection defined by $\psi : (i,j) \mapsto i + 3(j-1)$. Then using the equivalent action as defined above, the element $(\underline{g}, h)$ acts on Ω as follows.

B_1	B_2	B_3	B_4		B_1	B_3	B_4	B_2
1	4	7	10		2	7	10	5
2	5	8	11	$\mapsto$	1	8	12	6
3	6	9	12		3	9	11	4

The blocks are the sets of entries in each column, that is the subsets $\{1,2,3\}$, $\{4,5,6\}$, $\{7,8,9\}$, and $\{10,11,12\}$. Now if we let $\sigma : S_3 \wr S_4 \to S_{12}$ be the permutation representation as defined above, then $\sigma(\underline{g}, h)$ is the element $(1\,2)(3)(4\,7\,10\,5\,8\,12)(6\,9\,11)$ of S_{12}.

It can be shown that the imprimitive subgroup $\operatorname{Im}\sigma$ of S_n is a maximal imprimitive subgroup and furthermore such a maximal imprimitive subgroup is actually an (imprimitive) maximal subgroup of S_n.

There is a one-one correspondence between partitions of Ω into subsets of equal order and imprimitive maximal subgroups of S_n; for each proper divisor k of n, each partition of Ω into k subsets of order n/k is the block system for a unique imprimitive maximal subgroup (which is permutation isomorphic to $S_{n/k} \wr S_k$ acting imprimitively.)

When the context is clear we refer to a subgroup of S_n which is permutation isomorphic to $S_{n/k} \wr S_k$ acting imprimitively simply as a subgroup $S_{n/k} \wr S_k$ of S_n.

6.3 Bi-cycles in wreath products

The imprimitive action of $S_{n/k} \wr S_k$ on $\{1, \ldots, n/k\} \times \{1, \ldots, k\}$ naturally induces an action on the set of blocks. That is

$$B_j^{(\underline{g},h)} = B_{j^h} \text{ for } j \in \{1, \ldots, k\}, (\underline{g}, h) \in S_{n/k} \wr S_k.$$

Similarly, an imprimitive subgroup of S_n acts on a natural way on the set of blocks of Ω. So an element of an imprimitive subgroup of S_n induces an element of S_k, where k is the number of blocks. The element $(1\,2)(3)(4\,7\,10\,5\,8\,12)(6\,9\,11)$ of S_{12} in Example 6.2.1 induces the following permutation in the set of blocks

$$\{4, 5, 6\} \mapsto \{7, 8, 9\} \mapsto \{10, 11, 12\} \mapsto \{4, 5, 6\}$$

$$\{1, 2, 3\} \mapsto \{1, 2, 3\},$$

and hence a 3-cycle in S_4. This concept is used in the next lemma, which is stated without proof in [2].

Lemma 6.3.1. *Let n be a positive integer, and let M be an imprimitive maximal subgroup of S_n which is permutation isomorphic to $S_{n/k} \wr S_k$ acting imprimitively, where k is a non-trivial divisor of n. Let $g \in M$ be an $(r, n-r)$-cycle for a positive integer r such that $1 \leq r \leq n/2$. Then exactly one of the following cases occurs.*

1. *We have that $r = xn/k$ for a positive integer x, and the two orbits of g are unions of x and $k-x$ blocks, respectively. The permutation g induces an $(x, k-x)$-cycle in S_k.*

2. *We have that $r = yk$ for a positive integer y, one orbit of g intersects each block in a set of size y, and the other orbit of g intersects each block in a set of size $n/k - y$. The permutation g induces a k-cycle in S_k.*

An n-cycle in M always induces a k-cycle in S_k.

Proof. Let $g = (\omega_1 \dots \omega_n) \in M$ be an n-cycle. Note that $\omega_s^g = \omega_{s+1}$ if $1 \leq s \leq n-1$, and $\omega_n^g = \omega_1$. Since $k|n$, the permutation g^k maps $\omega_1 \mapsto \omega_{k+1} \mapsto \omega_{2k+1} \mapsto \dots \mapsto \omega_{(n/k-1)k+1} \mapsto \omega_1$, so the set $\{\omega_1, \omega_{k+1}, \dots, \omega_{(n/k-1)k+1}\}$ is an orbit of g^k on Ω. For $1 \leq l \leq k$, let

$$B_l = \{\omega_s \mid 1 \leq s \leq n \text{ and } s \equiv l \pmod{k}\}.$$

Then the sets B_l are the k orbits of g^k on Ω. Furthermore they are the blocks for M, and the natural action of g on the blocks

$$B_1 \mapsto \dots \mapsto B_k \mapsto B_1$$

induces a k-cycle in S_k.

Let $g = (\omega_1 \dots \omega_r)(\omega_{r+1} \dots \omega_n) \in M$, and let B_1 be the block for M containing ω_1. Let $\Delta = \{\omega_1 \dots \omega_r\}$, and note that for all l such that $1 \leq l \leq r$, we have $\omega_l = \omega_1^{g^{l-1}} \in B_1^{g^{l-1}}$. Let x be the largest integer such that $B_1, B_1^g, \dots, B_1^{g^{x-1}}$ are all distinct. Then $1 \leq x \leq k$, and $B_1^{g^x} = B_1$ (for if $B_1^{g^x} = B_1^{g^l}$ for some $0 < l < x$ then $B_1^{g^{x-l}} = B_1$). Also, for all l such that $1 \leq l \leq r$, we have $\omega_l \in B_1^{g^{l-l}} = B_1^{g^{l-1 \pmod{x}}}$. For $l \in \{2, \dots, x\}$ let $B_l = B_1^{g^{l-1}}$. Therefore $B_2, \dots, B_x$ are blocks, and $\Delta \subset B_1 \cup \dots \cup B_x$. It follows that $\Delta = (\Delta \cap B_1) \cup \dots \cup (\Delta \cap B_x)$, and this union is disjoint. Let $y = |\Delta \cap B_1|$, and note that $1 \leq y \leq n/k$. Since $\Delta \cap B_l = (\Delta \cap B_1)^{g^{l-1}}$, we have $|\Delta \cap B_l| = |\Delta \cap B_1| = y$ for $l \in \{1, \dots, x\}$, so $r = yx$.

First suppose that $B_1 \subseteq \Delta$, so $\Delta \cap B_l = B_l$ for $l \in \{1, \ldots, x\}$. Then Δ is the union of x blocks $B_1 \cup \ldots \cup B_x$, and $\Omega \setminus \Delta$ is the union of the remaining $k - x$ blocks. Also $y = |\Delta \cap B_1| = |B_1| = n/k$ so $r = xn/k$. Now let B_{x+1} be the block containing ω_{r+1}, and note that for all l such that $1 \leq l \leq n - r$, we have $\omega_{r+l} = \omega_{r+1}^{g^{l-1}} \in B_{x+1}^{g^{l-1}}$. Let z be the largest integer such that $B_{x+1}, B_{x+1}^{g}, \ldots, B_{x+1}^{g^{z-1}}$ are all distinct. Then $1 \leq z \leq n - k$, and $B_{x+1}^{g^z} = B_{x+1}$ (for if $B_{x+1}^{g^z} = B_{x+1}^{g^l}$ for some $0 < l < z$ then $B_{x+1}^{g^{z-l}} = B_{x+1}$). Also, for all l such that $1 \leq l \leq n-r$, we have $\omega_{r+l} \in B_{x+1}^{g^{l-l}} = B_{x+1}^{g^{l-1 \pmod z}}$. For $l \in \{2, \ldots, z\}$ let $B_{x+l} = B_{x+1}^{g^{l-1}}$. Therefore $\Omega \setminus \Delta \subset B_{x+1} \cup \ldots \cup B_{x+z}$, and it follows that $z = k - x$. The natural action of g on the blocks

$$B_1 \mapsto \ldots \mapsto B_x \mapsto B_1$$

$$B_{x+1} \mapsto \ldots \mapsto B_k \mapsto B_{x+1}$$

induces an $(x, k-x)$-cycle in S_k.

Now suppose that $B_1 \nsubseteq \Delta$, so $y < n/k$. We may assume that $\omega_{r+1} \in B_1$. Then $\omega_{r+l} \in B_1^{g^{l-1}} = B_1^{g^{l-1 \pmod x}}$ for $l \in \{1, \ldots, n-r\}$, so $\Omega \setminus \Delta \subset B_1 \cup \ldots \cup B_x$, and it follows that $x = k$ so $r = yk$. Furthermore $|\Delta \cap B_l| = y$ and $|(\Omega \setminus \Delta) \cap B_l| = n/k - y$ for $l \in \{1, \ldots, k\}$. The natural action of g on the blocks

$$B_1 \mapsto \ldots \mapsto B_k \mapsto B_1$$

induces a k-cycle in S_k.

□

If a bi-cycle in an imprimitive maximal subgroup of S_n satisfies the conditions of part 1 of Lemma 6.3.1 above, we say that it is *respectful.* If it satisfies the conditions of part 2 we say that it is *disrespectful.* We also say that an n-cycle in such a subgroup is *disrespectful* because it too induces a k-cycle in S_k. It follows directly from Lemma 6.3.1 that a bi-cycle can not be both respectful and disrespectful in a fixed imprimitive subgroup.

Example 6.3.1. Let $H = S_2 \wr S_5 < S_{10}$, and let the block system of H be $\{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{9,10\}\}$. Then the bi-cycle $(1\,3\,2\,4)(5\,7\,9\,6\,8\,10)$ is respectful, and induces a $(2,3)$-cycle in S_5. The bi-cycle $(9\,10)(1\,3\,5\,7\,2\,4\,6\,8)$ is also respectful, and induces a $(1,4)$-cycle in S_5. The bi-cycle $(1\,3\,5\,7\,9)(2\,4\,6\,8\,10)$ however is disrespectful and induces a 5-cycle in S_5.

For fixed subgroup $H = S_{n/k} \wr S_k$ of S_n, we define H_{resp} to be the set of all the respectful bi-cycles in H, and H_{dis} to be the set of all the disrespectful bi-cycles and the n-cycles in H. Since a fixed bi-cycle in H is not both respectful and disrespectful, it follows that $H_{\text{resp}} \cap H_{\text{dis}} = \emptyset$. The lemma which follows is the last in this section and involves counting bi-cycles.

Lemma 6.3.2. *Let H be an imprimitive maximal subgroup $S_{n/k} \wr S_k$ of S_n, and let $\Delta \subset \Omega$ be such that $d = |\Delta| \leq n/2$. If $C(\Delta) \cap H_{\text{resp}} \neq \emptyset$, then*

$$|C(\Delta) \cap H_{\text{resp}}| = (n/k)!^k (k/n)^2 (dk/n - 1)!(k - dk/n - 1)!.$$

If $C(\Delta) \cap H_{\text{dis}} \neq \emptyset$ and $d > 0$ then

$$|C(\Delta) \cap H_{\text{dis}}| = k!(d/k)!^k (n/k - d/k)!^k k/d(n - d).$$

If $C(\Delta) \cap H_{\text{dis}} \neq \emptyset$ and $d = 0$ then

$$|C(\Delta) \cap H_{\text{dis}}| = (k - 1)!(n/k)!^{k-1}(n/k - 1)!.$$

Proof. First suppose that $g \in C(\Delta) \cap H_{\text{resp}}$. Then $d > 0$ and g is a $(d, n-d)$-cycle, and by Lemma 6.3.1, Δ and $\Omega \setminus \Delta$ are a union of dk/n and $k - dk/n$ blocks of H respectively. To visualise this we represent H as an array

B_1	$\dots$	$B_{dk/n}$	$B_{dk/n+1}$	$\dots$	B_k
δ	$\dots$	δ	$*$	$\dots$	$*$
$\vdots$		$\vdots$	$\vdots$		$\vdots$
δ	$\dots$	δ	$*$	$\dots$	$*$

where the elements of Δ and $\Omega \setminus \Delta$ are represented by the symbols δ and $*$ respectively. We count the number of possibilities for g. Without loss of generality we may fix the first element of the first cycle of g. There are then $(dk/n-1)!$ ways of choosing the order of the $dk/n-1$ blocks from which to choose the next $dk/n-1$ elements of the first cycle. Within each of these blocks there are n/k choices of an element to pick, giving us altogether a further $(n/k)^{dk/n-1}$ choices. Now for the next dk/n elements of the first cycle we can chose from the remaining $n/k-1$ elements in each block - a total of $(n/k-1)^{dk/n}$ choices. Continuing in this manner, in total there are

$$(dk/n-1)!(n/k)^{dk/n-1}(n/k-1)^{dk/n}\ldots 1^{dk/n} = (dk/n-1)!(n/k)!^{dk/n}/(n/k)$$

possibilities for the first cycle of g. Using the same argument, but replacing dk/n by $k-(dk/n)$ where necessary (because the elements of the second cycle are taken from the $k-dk/n$ blocks of H containing the elements of $\Omega \setminus \Delta$) gives us a total of

$$(k-dk/n-1)!(n/k)!^{k-dk/n}/(n/k)$$

possibilities for the second cycle of g. Thus

$$\begin{aligned}|C(\Delta)\cap H_{\text{resp}}| = {} & [(dk/n-1)!(n/k)!^{dk/n}/(n/k)] \\ & \times [(k-dk/n-1)!(n/k)!^{k-dk/n}/(n/k)] \\ = {} & (n/k)!^{k}(k/n)^2(dk/n-1)!(k-dk/n-1)!.\end{aligned}$$

Now suppose that $g \in C(\Delta)\cap H_{\text{dis}}$ and $d>0$. So g is a $(d, n-d)$-cycle, but this time Δ and $\Omega \setminus \Delta$ have an intersection of size of d/k and $(n-d)/k$ respectively with each of the k blocks of H. This time the blocks of H are written

B_1	$\ldots$	B_k
δ	$\ldots$	δ
$\vdots$		$\vdots$
δ	$\ldots$	δ
$*$	$\ldots$	$*$
$\vdots$		$\vdots$
$*$	$\ldots$	$*$

Without loss of generality we may fix the first element of each cycle of g. There then are $(k-1)!$ ways of choosing the order of the $k-1$ blocks from which to chose the next $k-1$ elements of the first cycle. This then fixes the order in which the elements of the first cycle are taken from the blocks for H. Within each of these blocks there are d/k choices of an element to pick, giving us altogether a further $(d/k)^{k-1}$ choices. Now for the next k elements of the first cycle we can chose from the remaining $d/k-1$ elements from Δ in each block - a total of $(d/k-1)^k$ choices. Continuing in this manner, in total there are

$$(k-1)!(d/k)^{k-1}(d/k-1)^k \dots 1^k = (k-1)!(d/k)!^{k-1}(d/k-1)!$$

possibilities for the first cycle of g.

The order of the blocks from which we take the elements of the second cycle of g is fixed - it must be the same as that of the first cycle. The first element of the second cycle is fixed, but for the next $k-1$ elements, we have $n/k-d/k$ choices of which element of $\Omega \setminus \Delta$ to pick from each block. Thus we have altogether $(n/k-d/k)^{k-1}$ choices. For the next k elements we have $n/k-d/k-1$ choices, giving us altogether $(n/k-d/k-1)^k$ choices. Continuing in this manner, there are

$$(n/k-d/k)^{k-1}(n/k-d/k-1)^k \dots 1^k = (n/k-d/k)!^{k-1}(n/k-d/k-1)!$$

possibilities for the second cycle of g. Thus

$$\begin{aligned} |C(\Delta) \cap H_{\mathrm{dis}}| &= [(k-1)!(d/k)!^{k-1}(d/k-1)!] \\ &\qquad \times [(n/k-d/k)!^{k-1}(n/k-d/k-1)!] \\ &= k!(d/k)!^k(n/k-d/k)!^k k/d(n-d). \end{aligned}$$

Finally suppose that $g \in C(\Delta) \cap H_{\mathrm{dis}}$ and $d = 0$ (so g is an n-cycle). Without loss of generality we may fix the first element of g. There then are $(k-1)!$ ways of choosing the order of the $k-1$ blocks from which to chose the next $k-1$ elements of g. This then fixes the order in which the elements of g are taken from the blocks for H. Within each of these blocks there are n/k choices of an element to pick, giving us altogether a further $(n/k)^{k-1}$ choices. Now for the next k elements of g we can chose from the remaining $n/k-1$ elements in each block - a total of $(n/k-1)^k$ choices. Continuing in this manner, in total there are

$$(k-1)!(n/k)^{k-1}(n/k-1)^k \dots 1^k = (k-1)!(n/k)!^{k-1}(n/k-1)!$$

possibilities for g. Thus

$$|C(\Delta) \cap H_{\text{dis}}| = (k-1)!(n/k)!^{k-1}(n/k-1)!.$$

□

6.4 An upper bound

For a non-trivial divisor k of n, the set of subgroups of S_n which are permutation isomorphic to $S_{n/k} \wr S_k$ acting imprimitively is a conjugacy class of subgroups, which we denote by $\mathcal{H}_k$. This section concerns $\mathcal{H}_3$, which is non-empty when 3 divides n. When our result is combined with Lemmas 2.2.3 and 5.2.3 (to take into account the other imprimitive maximal subgroups of S_n), we get an explicit upper bound for the probability that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in any imprimitive maximal subgroup of S_n. We use this bound later for large values of n. Note that the proof of Lemma 6.4.1 is an adapted version of the proof of [2, Lemma 9]– our adaptation makes that result explicit.

Lemma 6.4.1. *Let n be a positive integer. For $i \in \{1,2\}$, let $\Delta_i \subset \Omega$, such that $|\Delta_i| \leq n/2$ and $\Delta_1 \neq \Delta_2$. Let g_{Δ_i} be selected uniformly and independently at random from $C(\Delta_i)$. Let E be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a subgroup from $\mathcal{H}_3$. Then*

$$Pr(E) < 3e^{10}n^4 2^{-\frac{4n}{3}}.$$

Proof. If 3 does not divide n, this probability is zero. Thus we may assume that 3 divides n. We write E_A for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a subgroup from $\mathcal{H}_3$, and that g_{Δ_2} is disrespectful in this group. We write E_B for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a subgroup from $\mathcal{H}_3$, and that g_{Δ_1} is disrespectful in this group. We write E_C for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a subgroup from $\mathcal{H}_3$, and that both g_{Δ_1} and g_{Δ_2} are respectful in this group. Then

$$E = E_A \cup E_B \cup E_C,$$

and so

$$Pr(E) \leq Pr(E_A) + Pr(E_B) + Pr(E_C).$$

First we find an upper bound for $Pr(E_A)$.

$$\begin{aligned} Pr(E_A) &\leq \sum_{H \in \mathcal{H}_3} Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ and } g_{\Delta_2} \text{ is disrespectful in } H.) \\ &= \sum_{H \in \mathcal{H}_3} Pr(g_{\Delta_1} \in H) \times Pr(g_{\Delta_2} \in H_{\text{dis}}) \\ &= \sum_{H \in \mathcal{H}_3} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H_{\text{dis}}|}{|C(\Delta_2)|} \\ &\leq \max_{H \in \mathcal{H}_3} \frac{|C(\Delta_2) \cap H_{\text{dis}}|}{|C(\Delta_2)|} \sum_{H \in \mathcal{H}_3} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|}. \end{aligned}$$

From Lemma 5.2.1 we know that a fixed bi-cycle or n-cycle is contained in at most n^2 conjugates of any subgroup of S_n, so

$$\sum_{H \in \mathcal{H}_3} |C(\Delta_1) \cap H| \leq n^2 |C(\Delta_1)|.$$

Substituting this we have

$$Pr(E_A) \leq n^2 \max_{H \in \mathcal{H}_3} \frac{|C(\Delta_2) \cap H_{\text{dis}}|}{|C(\Delta_2)|}.$$

Lemma 6.3.1 tells us that if $C(\Delta_2) \cap H_{\text{dis}} \neq \emptyset$, then $|\Delta_2| = 3y$ for some integer y such that $1 \leq y \leq n/6$. Then $|C(\Delta_2)| = (3y-1)!(n-3y-1)!$ and by Lemma 6.3.2,

$$|C(\Delta_2) \cap H_{\text{dis}}| = \frac{2\, y!^3 (n/3 - y)!^3}{y(n/3 - y)}.$$

Substituting again, we have

$$\begin{aligned} Pr(E_A) &\le n^2 \frac{2\,y!^3(n/3-y)!^3}{(3y-1)!(n-3y-1)!y(n/3-y)} \\ &= 18n^2 \frac{y!^3(n/3-y)!^3}{(3y)!(n-3y)!} \end{aligned}$$

We apply Stirling's formula as presented in Lemma 2.2.2.

$$\begin{aligned} Pr(E_A) &\le 18n^2 \frac{\left[\left(\frac{n/3-y}{e}\right)^{n/3-y}\sqrt{n/3-y}e^2\right]^3\left[\left(\frac{y}{e}\right)^y\sqrt{y}e^2\right]^3}{\left[\left(\frac{3y}{e}\right)^{3y}\sqrt{3y}e^{\frac{1}{2}}\right]\left[\left(\frac{n-3y}{e}\right)^{n-3y}\sqrt{n-3y}e^{\frac{1}{2}}\right]} \\ &\le 18e^{11}n^2\frac{y(n/3-y)}{3}3^{-n} \\ &= 6e^{11}n^2 3^{-n} y(n/3-y). \end{aligned}$$

Then finally since $y(n/3-y) \le n^2/36$ when $1 \le y \le \frac{n}{6}$, we have that

$$\begin{aligned} Pr(E_A) &\le e^{11}n^2 3^{-n} n^2/6 \\ &\le e^{10}n^4 3^{-n}. \end{aligned}$$

If we apply exactly the same argument but with Δ_1 and Δ_2 exchanged, we obtain the same upper bound for $Pr(E_B)$.

Now we find an upper bound for $Pr(E_C)$. Let $H \in \mathcal{H}_3$ be such that H contains respectful bi-cycles from both Δ_1 and Δ_2, and let g be a bi-cycle from $C(\Delta_1) \cap H_{\text{resp}}$. By Lemma 6.3.1 we have that $|\Delta_1| = n/3$ and Δ_1 is a union of blocks of Ω under the action of H. Since there are three blocks of order $n/3$, Δ_1 is one of the blocks. The same argument applies to Δ_2, and since $\Delta_1 \ne \Delta_2$, the blocks must be Δ_1, Δ_2, and $\Omega \setminus (\Delta_1 \cup \Delta_2)$. Thus H is completely determined by Δ_1 and Δ_2 and

$$\begin{aligned} Pr(E_C) &= \Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ and both are respectful in } H) \\ &= \Pr(g_{\Delta_1} \in H_{\text{resp}}) \times \Pr(g_{\Delta_2} \in H_{\text{resp}}) \\ &= \frac{|C(\Delta_1) \cap H_{\text{resp}}|}{|C(\Delta_1)|}\frac{|C(\Delta_2) \cap H_{\text{resp}}|}{|C(\Delta_2)|}. \end{aligned}$$

Now for $i \in \{1,2\}$, $|C(\Delta_i)| = (n/3-1)!(2n/3-1)!$, and by Lemma 6.3.2, $|C(\Delta_i) \cap H_{\text{resp}}| = (n/3-1)!^2(n/3)!$. Therefore

$$\begin{aligned} Pr(E_C) &= \left[\frac{\frac{n}{3}!\left(\frac{n}{3}-1\right)!}{\left(\frac{2n}{3}-1\right)!} \right]^2 \\ &= \left[\frac{\left(\frac{n}{3}\right)!^2\left(\frac{2n}{3}\right)}{\left(\frac{2n}{3}\right)!\left(\frac{n}{3}\right)} \right]^2. \end{aligned}$$

Again by Stirling's formula, it follows that

$$\begin{aligned} Pr(E_C) &\leq \left[2\left(\left(\frac{n}{3e}\right)^{\frac{n}{3}} \sqrt{\frac{n}{3}} e^2 \right)^2 \left(\frac{3e}{2n}\right)^{\frac{2n}{3}} \sqrt{\frac{3}{2n}} e^{-\frac{1}{2}} \right]^2 \\ &= \frac{2e^7 n}{3.2^{\frac{4n}{3}}} \\ &\leq e^7 n 2^{-\frac{4n}{3}}. \end{aligned}$$

Combining our upper bounds, and using the inequality $3^{-n} < 2^{-\frac{4n}{3}}$ gives

$$\begin{aligned} Pr(E) &\leq e^{10} n^4 3^{-n} + e^{10} n^4 3^{-n} + e^7 n 2^{-\frac{4n}{3}} \\ &\leq 3e^{10} n^4 2^{-\frac{4n}{3}}. \end{aligned}$$

Our result follows. □

6.5 A tighter upper bound

Recall that n is a positive integer, and $\Delta_1, \Delta_2 \subset \Omega$ such that $|\Delta_1|, |\Delta_2| \leq n/2$, and $\Delta_1 \neq \Delta_2$. Also, g_{Δ_j} is selected uniformly and independently at random from $C(\Delta_j)$. Define E_{imprim} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroups of S_n.

The result in our previous section, when combined with Lemmas 2.2.3 and 5.2.3 (to take into account the other imprimitive maximal subgroups of S_n), we get an explicit upper bound for $Pr(E_{imprim})$, which we use later for large values of n. This bound however, is too high to be of use for medium and small values of n. Now we develop the theory which allows us to calculate a tighter (but much more complicated) upper bound. Recall that for a fixed non-trivial divisor k of n, $\mathcal{H}_k$ is the conjugacy class of subgroups of S_n which are permutation isomorphic to $S_{n/k} \wr S_k$ acting imprimitively.

By Lemma 5.1.1 we have

$$
\begin{aligned}
Pr(E_{imprim}) &\leq \sum_{\substack{k|n \\ k\neq 1,n}} \sum_{H\in\mathcal{H}_k} \frac{|C(\Delta_1)\cap H|}{|C(\Delta_1)|}\frac{|C(\Delta_2)\cap H|}{|C(\Delta_2)|} \\
&= \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{\substack{k|n \\ k\neq 1,n}} \sum_{H\in\mathcal{H}_k} |C(\Delta_1)\cap H||C(\Delta_2)\cap H|.
\end{aligned}
$$

Let k be a fixed non-trivial divisor of n. The results in this section give an upper bound for

$$\sum_{H\in\mathcal{H}_k} |C(\Delta_1)\cap H||C(\Delta_2)\cap H|.$$

The total number of subgroups $H \in \mathcal{H}_k$ which contain permutations from both $C(\Delta_1)$ and $C(\Delta_2)$ is $h_1 + h_2 + h_3 + h_4$, where

$$
\begin{aligned}
h_1 &= |\{H : H \in \mathcal{H}_k \text{ such that } C(\Delta_1)\cap H_{\text{resp}} \neq \emptyset \text{ and } C(\Delta_2)\cap H_{\text{resp}} \neq \emptyset\}|, \\
h_2 &= |\{H : H \in \mathcal{H}_k \text{ such that } C(\Delta_1)\cap H_{\text{resp}} \neq \emptyset \text{ and } C(\Delta_2)\cap H_{\text{dis}} \neq \emptyset\}|, \\
h_3 &= |\{H : H \in \mathcal{H}_k \text{ such that } C(\Delta_1)\cap H_{\text{dis}} \neq \emptyset \text{ and } C(\Delta_2)\cap H_{\text{resp}} \neq \emptyset\}|, \\
h_4 &= |\{H : H \in \mathcal{H}_k \text{ such that } C(\Delta_1)\cap H_{\text{dis}} \neq \emptyset \text{ and } C(\Delta_2)\cap H_{\text{dis}} \neq \emptyset\}|.
\end{aligned}
$$

It follows from the definitions of the h_i that

$$
\begin{aligned}
\sum_{H\in\mathcal{H}_k} |C(\Delta_1)\cap H||C(\Delta_2)\cap H| = {}& h_1 \times |C(\Delta_1)\cap H_{\text{resp}}| \times |C(\Delta_2)\cap H_{\text{resp}}| \\
&+ h_2 \times |C(\Delta_1)\cap H_{\text{resp}}| \times |C(\Delta_2)\cap H_{\text{dis}}| \\
&+ h_3 \times |C(\Delta_1)\cap H_{\text{dis}}| \times |C(\Delta_2)\cap H_{\text{resp}}| \\
&+ h_4 \times |C(\Delta_1)\cap H_{\text{dis}}| \times |C(\Delta_2)\cap H_{\text{dis}}|.
\end{aligned}
$$

In Lemma 6.3.2 we gave expressions for $|C(\Delta_i)\cap H_{\text{resp}}|$ and $|C(\Delta_i)\cap H_{\text{dis}}|$ in terms of n, k and d_i. We now do the same for the h_i. In Section 6.2 we observed that there is a one-one correspondence between subgroups $H \in \mathcal{H}_k$

and partitions of Ω into k subsets of order n/k. The partition is a system of blocks for the subgroup - each part is a block. We count suitable partitions to determine h_1, h_2, h_3 and h_4.

First we define two functions of non-negative integer variables x and y. For $x > 0$, define $p(x, y)$ to be the number of partitions of a set of size x into subsets of size y, and $op(x, y)$ to be the number of ordered partitions of a set of size x into subsets of size y. Define $p(0, y) = op(0, y) = 1$. The next result is standard so is stated without proof.

Lemma 6.5.1. *Let x and y be non-negative integers, and define $p(x, y)$ and $op(x, y)$ as above. Then*

$$p(x,y) = \begin{cases} \frac{x!}{y!^{x/y}(x/y)!} & \text{if } x > 0 \text{ and } y \mid x, \\ 0 & \text{if } x > 0 \text{ and } y \nmid x, \\ 1 & \text{if } x = 0. \end{cases}$$

$$op(x,y) = \begin{cases} \frac{x!}{y!^{x/y}} & \text{if } x > 0 \text{ and } y \mid x, \\ 0 & \text{if } x > 0 \text{ and } y \nmid x, \\ 1 & \text{if } x = 0. \end{cases}$$

Let $d_1 = |\Delta_1|$, $d_2 = |\Delta_2|$ and $i = |\Delta_1 \cap \Delta_2|$. Note that $i \le \min(d_1, d_2)$ and if $d_1 = d_2$ then $i \le d_1 - 1$.

Lemma 6.5.2. *Let h_1, h_2 and h_3 be as defined above. If $d_1, d_2 > 0$, then*

$$h_1 = p(i, n/k) \times p(d_1 - i, n/k) \times p(d_2 - i, n/k) \times p(n + i - d_1 - d_2, n/k),$$

otherwise $h_1 = 0$. If $d_1 > 0$ and $i = d_1 d_2/n$, then

$$h_2 = p(d_1 - i, (n - d_2)/k) \times op(i, d_2/k) \times p(n + i - d_1 - d_2, (n - d_2)/k) \times op(d_2 - i, d_2/k),$$

otherwise $h_2 = 0$. If $d_2 > 0$ and if $i = d_1 d_2/n$, then

$$h_3 = p(d_2 - i, (n - d_1)/k) \times op(i, d_1/k) \times p(n + i - d_1 - d_2, (n - d_1)/k) \times op(d_1 - i, d_1/k),$$

otherwise $h_3 = 0$.

Proof. We apply Lemma 6.3.1. For a fixed $H \in \mathcal{H}_k$, if $C(\Delta_1) \cap H_{\text{resp}} \neq \emptyset$ and $C(\Delta_2) \cap H_{\text{resp}} \neq \emptyset$, then Δ_1 is a union of d_1k/n blocks for H, and Δ_2 is a union of d_2k/n blocks. Consequently $\Delta_1 \cap \Delta_2$ must be a union of ik/n blocks, and $\Omega \setminus (\Delta_1 \cap \Delta_2)$ must be a union of $(n + i - d_1 - d_2)k/n$ blocks. Therefore each subgroup counted in h_1 corresponds to a partition $\{B_1, \ldots, B_k\}$ of Ω such that:

1. $|B_i| = n/k$;
2. $B_1 \cup \ldots \cup B_{ik/n} = \Delta_1 \cap \Delta_2$;
3. $B_{ik/n+1} \cup \ldots \cup B_{d_1k/n} = \Delta_1 \setminus \Delta_1 \cap \Delta_2$;
4. $B_{d_1k/n+1} \cup \ldots \cup B_{(d_1+d_2-i)k/n} = \Delta_2 \setminus \Delta_1 \cap \Delta_2$.

Such a partition is represented below. The i elements of $\Delta_1 \cap \Delta_2$ are all represented by the symbol δ_{12}, the $d_1 - i$ elements of $\Delta_1 \setminus (\Delta_1 \cap \Delta_2)$ by the symbol δ_1, the $d_2 - i$ elements of $\Delta_2 \setminus (\Delta_1 \cap \Delta_2)$ by the symbol δ_2, and the $n + i - d_1 - d_2$ elements of $\Omega \setminus (\Delta_1 \cup \Delta_2)$ are represented by the symbol $*$.

B_1	$\ldots$	$B_{\frac{ik}{n}}$		$\ldots$	$B_{\frac{d_1k}{n}}$		$\ldots$	$B_{\frac{(d_1+d_2-i)k}{n}}$		$\ldots$	B_k
δ_{12}	$\ldots$	δ_{12}	δ_1	$\ldots$	δ_1	δ_2	$\ldots$	δ_2	$*$	$\ldots$	$*$
$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
δ_{12}	$\ldots$	δ_{12}	δ_1	$\ldots$	δ_1	δ_2	$\ldots$	δ_2	$*$	$\ldots$	$*$

The number of such partitions is

$$h_1 = p(i, n/k) \times p(d_1 - i, n/k) \times p(d_2 - i, n/k) \times p(n + i - d_1 - d_2, n/k).$$

Now we consider h_2. If $d_1 = 0$ then $C(\Delta_1)$ is the set of n-cycles, which by definition are disrespectful in any imprimitive maximal subgroup, so $h_2 = 0$. If $d_1 > 0$ we apply Lemma 6.3.1 again. For a fixed $H \in \mathcal{H}_k$, if $C(\Delta_1) \cap H_{\text{resp}} \neq \emptyset$ and $C(\Delta_2) \cap H_{\text{dis}} \neq \emptyset$, then Δ_1 must be a union of d_1k/n blocks for H, but this time the intersection of Δ_2 with each of the blocks must be of order d_2/k. It follows that the order of the intersection of $\Delta_1 \cap \Delta_2$ with each of the blocks is either 0 or d_2/k, and $i = (d_1k/n) \times (d_2/k) = d_1d_2/n$. Each subgroup counted in h_2 corresponds to a partition $\{B_1, \ldots, B_k\}$ of Ω such that:

1. $|B_j| = n/k$;
2. $B_1 \cup \ldots \cup B_{d_1k/n} = \Delta_1$;
3. $|B_j \cap \Delta_2| = d_2/k$ for $j \in \{1, \ldots, k\}$.

Again, see the representation below.

B_1	$\ldots$	$B_{d_1k/n}$	$B_{d_1k/n+1}$	$\ldots$	B_k
δ_{12}	$\ldots$	δ_{12}	δ_2	$\ldots$	δ_2
$\vdots$		$\vdots$	$\vdots$		$\vdots$
δ_{12}	$\ldots$	δ_{12}	δ_2	$\ldots$	δ_2
δ_1	$\ldots$	δ_1	$*$	$\ldots$	$*$
$\vdots$		$\vdots$	$\vdots$		$\vdots$
δ_1	$\ldots$	δ_1	$*$	$\ldots$	$*$

To count the number of such partitions, first we look at the d_1k/n blocks which contain the elements of Δ_1. Each of these blocks contains d_2/k elements of $\Delta_1 \cap \Delta_2$ and $(n-d_2)/k$ elements of $\Delta_1 \setminus (\Delta_1 \cap \Delta_2)$. There are $p(d_1-i, (n-d_2)/k)$ ways of assigning the $d_1 - i$ elements of $\Delta_1 \setminus (\Delta_1 \cap \Delta_2)$ (note that $d_1 - i > 0$, since $d_1 > 0$ and $i = d_1d_2/n < d_1$). This fixes these blocks, and there are then $op(i, d_2/k)$ ways of assigning the remaining elements of these blocks (that is the elements of $\Delta_1 \cap \Delta_2$). In total there are $p(d_1 - i, (n - d_2)/k) \times op(i, d_2/k)$ possibilities for these first d_1k/n blocks. By a similar argument, the elements of $\Omega \setminus \Delta_1$ can be assigned in $p(n + i - d_1 - d_2, (n - d_2)/k) \times op(d_2 - i, d_2/k)$ ways, and so the total number h_2 is the product of these two numbers.

The same argument with Δ_1 and Δ_2 exchanged gives us our expression for h_3. □

We extend the definition of the functions p and op to include the case where y is a list of non-negative integers $y_1, \ldots, y_k$. For $x > 0$ define $p(x, [y_1, \ldots, y_k])$ to be the number of partitions of a set of order x into k subsets of orders

$y_1, \ldots, y_k$, and $op(x, [y_1, \ldots, y_k])$ to be the number of ordered partitions of a set of order x into k subsets of orders $y_1, \ldots, y_k$. Define $p(0, [y_1, \ldots, y_k]) = op(0, [y_1, \ldots, y_k]) = 1$. Again the next result is standard so is stated without proof.

Lemma 6.5.3. *Let $y_1, \ldots, y_k$ and x be non-negative integers. Define $p(x, [y_1, \ldots, y_k])$ and $op(x, [y_1, \ldots, y_k])$ as above. If m_l is the number of times the integer l appears in the list $[y_1, \ldots, y_k]$, then*

$$\begin{aligned} p(x, [y_1, \ldots, y_k]) &= \begin{cases} \frac{x!}{y_1! \ldots y_k! m_1! \ldots m_x!} & \textit{if } x > 0 \textit{ and } \sum_{j=1}^{k} y_j = x; \\ 0 & \textit{if } x > 0 \textit{ and } \sum_{j=1}^{k} y_j \neq x; \\ 1 & \textit{if } x = 0. \end{cases} \\ op(x, [y_1, \ldots, y_k]) &= \begin{cases} \frac{x!}{y_1! \ldots y_k!} & \textit{if } x > 0 \textit{ and } \sum_{j=1}^{k} y_j = x; \\ 0 & \textit{if } x > 0 \textit{ and } \sum_{j=1}^{k} y_j \neq x; \\ 1 & \textit{if } x = 0. \end{cases} . \end{aligned}$$

Now we consider h_4. For a fixed $H \in \mathcal{H}_k$, if $C(\Delta_1) \cap H_{\text{dis}} \neq \emptyset$ and $C(\Delta_2) \cap H_{\text{dis}} \neq \emptyset$, then by Lemma 6.3.1 the intersection of Δ_1 and Δ_2 with each of the k blocks for H must be of order d_1/k and d_2/k respectively. Therefore the order of the intersection of $\Delta_1 \cap \Delta_2$ with each of the blocks for H is at most $\min(d_1, d_2)/k$, but the orders of these intersections are not necessarily all the same. We write a decreasing list of the orders, and we call this list the *shape* of the intersection. We illustrate this concept with an example.

Example 6.5.1. Let $n = 18$, $d_1 = 9$, $d_2 = 6$ and $i = 3$. Let $k = 3$, so then h_4 is the number of subgroups $H \in \mathcal{H}_3$ such that $C(\Delta_1) \cap H_{\text{dis}} \neq \emptyset$ and $C(\Delta_2) \cap H_{\text{dis}} \neq \emptyset$. Let H be such a subgroup, and let B_1, B_2, B_3 be the blocks for H. Then $|B_j \cap \Delta_1| = 9/3 = 3$, $|B_i \cap \Delta_2| = 6/3 = 2$, and $0 \leq |B_j \cap \Delta_1 \cap \Delta_2| \leq 2$. There are two possible shapes of $\Delta_1 \cap \Delta_2$ - they are

$[2,1,0]$ and $[1,1,1]$, as represented below.

B_1	B_2	B_3
δ_{12}	δ_{12}	δ_1
δ_{12}	δ_1	δ_1
δ_1	δ_1	δ_1
$*$	δ_2	δ_2
$*$	$*$	δ_2
$*$	$*$	$*$

B_1	B_2	B_3
δ_{12}	δ_{12}	δ_{12}
δ_1	δ_1	δ_1
δ_1	δ_1	δ_1
δ_2	δ_2	δ_2
$*$	$*$	$*$
$*$	$*$	$*$

Let $m = \min(d_1, d_2)/k$ and define

$$\mathcal{I} = \{[y_1, \ldots, y_k] : y_j \text{ integers such that } m \geq y_1 \geq \ldots \geq y_k \geq 0 \text{ and } \sum_{j=1}^{k} y_j = i\}.$$

The set $\mathcal{I}$ contains all possible shapes of $\Delta_1 \cap \Delta_2$ for a fixed subgroup in $\mathcal{H}_k$.

Lemma 6.5.4. *Let h_4 and $\mathcal{I}$ be as defined above. For $[y_1, \ldots, y_k] \in \mathcal{I}$, let m_0 be the number of zeros in the list $[y_1, \ldots, y_k]$. Then*

$$\begin{aligned} h_4 = \sum_{[y_1,\ldots,y_k]\in\mathcal{I}} & p(i, [y_1, \ldots, y_k]) \\ & \times op(n + i - d_1 - d_2, [y_1 + (n - d_1 - d_2)/k, \ldots, y_k + (n - d_1 - d_2)/k]) \\ & \times\ op(d_1 - i, [d_1/k - y_1, \ldots, d_1/k - y_k]) \\ & \times\ op(d_2 - i, [d_2/k - y_1, \ldots, d_2/k - y_k]))\ /m_0! \end{aligned}$$

Proof. h_4 is the number of partitions $\{B_1, \ldots, B_k\}$ of Ω such that:

1. $|B_j| = n/k$;

2. $|B_j \cap \Delta_1| = d_1/k$ for $j \in \{1, \ldots, k\}$.

3. $|B_j \cap \Delta_2| = d_2/k$ for $j \in \{1, \ldots, k\}$.

Such a partition is represented in the figure below. For a fixed shape $[y_1, \ldots, y_k] \in \mathcal{I}$ we count the number of partitions of Ω which satisfy our three conditions above, and have $\Delta_1 \cap \Delta_2$ of this shape. We do this by first counting the number of unordered partitions of $\Delta_1 \cap \Delta_2$ into sets of order

B_1	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	B_k
δ_{12}	$\dots$	δ_{12}	$\dots$	δ_{12}	$\dots$	δ_{12}
				$\vdots$		$\vdots$
$\vdots$		$\vdots$		δ_{12}	$\dots$	δ_{12}
				δ_1	$\dots$	δ_1
δ_{12}	$\dots$	δ_{12}				
δ_1	$\dots$	δ_1		$\vdots$		$\vdots$
$\vdots$		$\vdots$				
δ_1	$\dots$	δ_1	$\dots$	δ_1	$\dots$	δ_1
δ_2	$\dots$	δ_2	$\dots$	δ_2	$\dots$	δ_2
$\vdots$		$\vdots$				
δ_2	$\dots$	δ_2		$\vdots$		$\vdots$
$*$	$\dots$	$*$				
				δ_2	$\dots$	δ_2
$\vdots$		$\vdots$		$*$	$\dots$	$*$
				$\vdots$		$\vdots$
$*$	$\dots$	$*$	$\dots$	$*$	$\dots$	$*$

$y_1, \dots, y_k$. This fixes $k - m_0$ of the blocks, where m_0 is the number of zeros in the list $[y_1, \dots, y_k]$. We then multiply by the number of ordered partitions of $\Delta_1 \setminus (\Delta_1 \cap \Delta_2)$ into sets of order $d_1/k - y_1, \dots, d_1/k - y_k$, and divide by $m_0!$ which fixes the remaining blocks. As the blocks are now fixed, we multiply by the number of ordered partitions of $\Delta_2 \setminus (\Delta_1 \cap \Delta_2)$ and $\Omega \setminus (\Delta_1 \cup \Delta_2)$ into sets of the appropriate orders. Finally we sum this expression over all shapes in $\mathcal{I}$ to give h_4. $\square$

Now, since

$$Pr(E_{imprim}) \leq \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{\substack{k|n \\ k \neq 1,n}} \sum_{H \in \mathcal{H}_k} |C(\Delta_1) \cap H||C(\Delta_2) \cap H|,$$

and for a fixed divisor k of n we have

$$\begin{aligned}\sum_{H\in\mathcal{H}_k}|C(\Delta_1)\cap H||C(\Delta_2)\cap H| = h_1 &\times |C(\Delta_1)\cap H_{\mathrm{resp}}|\times|C(\Delta_2)\cap H_{\mathrm{resp}}|\\ &+ h_2\times|C(\Delta_1)\cap H_{\mathrm{resp}}|\times|C(\Delta_2)\cap H_{\mathrm{dis}}|\\ &+ h_3\times|C(\Delta_1)\cap H_{\mathrm{dis}}|\times|C(\Delta_2)\cap H_{\mathrm{resp}}|\\ &+ h_4\times|C(\Delta_1)\cap H_{\mathrm{dis}}|\times|C(\Delta_2)\cap H_{\mathrm{dis}}|,\end{aligned}$$

we have an upper bound for $Pr(E_{imprim})$ in terms of n, k, d_1, d_2 and i. We will use this upper bound later in our `GAP` programs for small and medium values of n.

Chapter 7

Primitive maximal subgroups

The O'Nan-Scott theorem classifies maximal subgroups of S_n. For odd values of n we use this classification, together with another well known result, to sort primitive maximal subgroups of S_n into types*. Then we determine an explicit upper bound for the number of conjugacy classes of each type (these bounds also apply when n is even). We summarise the bounds in Table 7.1 at the end of the chapter.*

7.1 Sorting into types

The O'Nan-Scott theorem is stated in the preliminaries chapter (see Theorem 2.1.3). It says that maximal subgroups of the symmetric group belong to one of the following classes: intransitive, transitive imprimitive, primitive non-basic, affine, diagonal, almost simple. The next result allows us to subdivide the class of almost simple maximal subgroups. First we define the subspace subgroups and the (primitive) subspace actions of an almost simple group with classical socle. This definition is taken from [16].

Let H be a finite almost simple group, that has classical socle T and naturally associated vector space V over a field of characteristic p. Let K be a maximal subgroup of H. Then K is a *subspace subgroup* if one of the following holds:

(1) $K = G_U$ for some proper non-zero subspace U of V, where U is totally singular, non-degenerate, or, if H is orthogonal and $p = 2$, a non-singular 1-dimensional space (U is any subspace if $T = PSL(V)$);

(2) $T = PSL(V)$, H contains a graph automorphism of T, and $K = G_{U,W}$ where U, W are proper non-zero subspaces of V, dim V = dim U+dim W and either $U \leq W$ or $U \cap W = 0$;

(3) $T = Sp_{2m}(q)$, $p = 2$ and $K \cap T = O^{\pm}_{2m}(q)$.

A *subspace action* of H is the action of H on the set of cosets $[H : K]$, where K is a subspace subgroup of H.

Theorem 7.1.1. [14, Proposition 2] *Let H be an almost simple primitive subgroup of S_n, and let $T = \operatorname{soc} H$. Then one of the following holds:*

1. *$T = A_m$ acting on the k-subsets of $\{1, \ldots, m\}$, or on partitions of $\{1, \ldots, m\}$ into l sets of size k, where $m = kl$, $k > 1$, $l > 1$; $n = \binom{m}{k}$ or $m!/k!^l l$ respectively;*

2. *T is a classical simple group and H is acting on subspaces;*

3. *$H = M_{23}$ or M_{24} and $n = 23$ or 24 respectively;*

4. *$|H| < n^5$.*

We now consider odd positive integers only, and combine Theorem 2.1.3 and Theorem 7.1.1.

Theorem 7.1.2. *Let n be an odd positive integer, such that $n \neq 23$. Let M be a primitive maximal subgroup of S_n other than A_n. Then M is one of the following:*

1. *S_m, for some integer $m \leq n - 1$, acting on the set of k-subsets of $\{1, \ldots, m\}$ for some integer k such that $2 \leq k \leq m - 1$, or on the*

set of partitions of $\{1, \ldots, m\}$ *into* k*-subsets, for some proper divisor* k *of* m*;*

2. *An almost simple group (with classical socle) acting on subspaces;*

3. *An almost simple group of order at most* n^5*;*

4. $S_k \wr S_{\log_k n}$ *(acting primitively), for some integer* k *such that* n *is a power of* k*;*

5. $\mathrm{AGL}(\log_p n, p)$ *acting on a vector space of dimension* $\log_p n$ *over* $\mathbb{F}_p$*, for a prime* p *such that* n *is a power of* p*.*

Proof. Suppose that M is in class 6 (almost simple) of the O'Nan-Scott Theorem. Then $\operatorname{soc} M$ satisfies the hypotheses of Theorem 7.1.1. If $\operatorname{soc} M$ is in part 1 of Theorem 7.1.1, then for some fixed integer m we have that $\operatorname{soc} M$ is permutation isomorphic to A_m acting (in the natural way) on the set of k-subsets of $\{1, \ldots, m\}$ for some integer k such that $2 \leq k \leq m-1$, or on the set of partitions of $\{1, \ldots, m\}$ into k-subsets, for some proper divisor k of m. Furthermore since M is almost simple, we have $A_m = \operatorname{soc} M \leq M \leq \mathrm{Aut}(A_m) = S_m$, and if A_m acts in this way with degree n then so does S_m. Then by maximality of M we must have that $M \cong S_m$. Clearly $m \leq n - 1$.

If M is in class 5 (diagonal) of the O'Nan-Scott Theorem, then $n = |T|^{k-1}$ where T is a nonabelian finite simple group, and k is an integer such that $k \geq 2$. However, by Theorem 2.1.7, the order of a nonabelian finite simple group is even. So $|T|$ is even which contradicts our hypothesis that n is odd. So class 5 of the O'Nan-Scott Theorem is ruled out. □

For any positive integer n, if a maximal subgroup M of S_n is in part i of the theorem above, we say that M is a maximal subgroup of *type* i. For example, $\mathrm{AGL}(1, 5)$ is a type 5 maximal subgroup of S_5. Note that although Theorem 7.1.2 is concerned with odd values of n only, the remainder of this chapter applies to all positive values of n.

For $i \in \{1, \ldots, 5\}$, let

$$\begin{aligned} M_i &= \{M : M \leq S_n,\ M \text{ maximal},\ M \text{ is of type i}\}, \text{ and} \\ \mathcal{M}_i &= \{[M]_{S_n} : M \in M_i\}. \end{aligned}$$

So M_i is the set of type i maximal subgroups of S_n, and $\mathcal{M}_i$ is the set of conjugacy classes of such subgroups. Our goal in this chapter is to find explicit upper bounds for each $|\mathcal{M}_i|$. First we deal with $\mathcal{M}_4$ and $\mathcal{M}_5$ as these are the easiest cases.

If n is a proper power of an integer k such that $k \geq 2$, then there is precisely one primitive action of the wreath product $S_k \wr S_{\log_k n}$ on a set of size n (up to equivalence), so by Lemma 2.1.2 there is one conjugacy class of subgroups of S_n which are permutation isomorphic to this action. Since $k \geq 2$ we have $\log_k n \leq \log_2 n$. Thus $|\mathcal{M}_4| \leq \log_2 n$.

Similarly, if n is a power of a prime p, there is precisely one (natural) action of the affine group $\mathrm{AGL}(\log_p n, p)$ on a vector space of dimension $\log_p n$ over $\mathbb{F}_p$ (up to equivalence). For a fixed n, there is at most one prime p of which n is a power, thus $|\mathcal{M}_5| \leq 1$.

Types $1, 2$ and 3 are more difficult. For a fixed (abstract) group G, Lemma 2.1.2 provides us with methods of finding an upper bound for the number of conjugacy classes of transitive subgroups of S_n which are isomorphic to G. We use these methods to arrive at our upper bounds for $|\mathcal{M}_1|$, $|\mathcal{M}_2|$ and $|\mathcal{M}_3|$.

7.2 Type 1 primitive maximal subgroups

Lemma 7.2.1. *We have that*

$$|\mathcal{M}_1| < n^2.$$

Let $M \in M_1$, so $M \cong S_m$ for an integer m such that $m \leq n - 1$.

Suppose that M is permutation isomorphic to S_m acting (in the natural way) on the set of k-subsets of $\{1, \ldots, m\}$ for some integer $2 \leq k \leq m-2$. Then $n = \binom{m}{k}$ since this is the number of such k-subsets. For fixed m and n, there is at most one integer k such that $1 \leq k \leq m/2$ which satisfies this equation, k_o say, and then clearly $m - k_o$ is the only other solution (if $k_0 = m/2$ these solutions are the same). So M is permutation isomorphic to S_m acting on the set of k_o-subsets of $\{1, \ldots, m\}$, or the set of $(m-k_o)$-subsets of $\{1, \ldots, m\}$. However these two actions of S_m are equivalent. So there is at most one such action of S_m (up to equivalence).

Now suppose that M is permutation isomorphic to S_m acting (in the natural way) on the set of partitions of $\{1, \ldots, m\}$ into k-subsets, for some proper divisor k of m. Then $2 \leq k \leq m-1$, and so there are most $m-2$ such actions of S_m. (In fact $n = \frac{m!}{k!^{(m/k)}(m/k)!}$, since this is the number of such partitions, and for fixed m and n, we conjecture that there are at most two solutions to this equation, so there are at most two such actions. However this is not proved here.)

Thus M is permutation isomorphic to S_m acting in one of at most $1+(m-2) = m-1$ non equivalent ways. So for each $m \leq n-1$, by Lemma 2.1.2 there are at most $m-1$ conjugacy classes of groups in M_1 which are isomorphic to S_m.

Thus in total

$$|\mathcal{M}_1| \leq \sum_{m=2}^{n-1} (m-1) = \frac{(n-1)(n-2)}{2} < n^2.$$

7.3 Type 2 primitive maximal subgroups

The next lemma is useful for counting conjugacy classes of type 2 and 3 maximal subgroups.

Lemma 7.3.1. *Let n be a positive integer. Except for A_n, every maximal subgroup of S_n is the normaliser of its socle.*

Proof. For any subgroup G of S_n, we have

$$\operatorname{soc} G \trianglelefteq G \leq N_{S_n}(\operatorname{soc} G) \leq S_n.$$

Let M be a maximal subgroup of S_n other than A_n. Since $\operatorname{soc} M \neq A_n$, it follows that $\operatorname{soc} M \ntrianglelefteq S_n$, so $N_{S_n}(\operatorname{soc} M) < S_n$. Then by maximality of M we have $M = N_{S_n}(\operatorname{soc} M)$. That is, M is the normaliser in S_n of $\operatorname{soc} M$. $\square$

Now we define a set of subgroups and a corresponding set of conjugacy classes of these subgroups.

$$\begin{aligned} T_{cl} &= \{T : T \leq S_n, T \text{ is a classical simple group,} \\ &\quad T \text{ is the socle of an almost simple group acting on subspaces}\}, \text{ and} \\ \mathcal{T}_{cl} &= \{[T]_{S_n} : T \in T_{cl}\}. \end{aligned}$$

Lemma 7.3.2. *We have that*

$$|\mathcal{M}_2| \leq |\mathcal{T}_{cl}|.$$

Proof. Let f be the map $f : \mathcal{M}_2 \to \mathcal{T}_{cl}$ defined by

$$f : [M]_{S_n} \mapsto [\operatorname{soc} M]_{S_n} \qquad M \in M_2.$$

We first show that f is well-defined. Let $G_1, G_2 \in M_2$ and suppose that $[G_1]_{S_n} = [G_2]_{S_n}$. Then $G_1 = g^{-1}G_2g$ for some $g \in S_n$ and so $\operatorname{soc} G_1 = g^{-1}\operatorname{soc} G_2 g$ and $[\operatorname{soc} G_1]_{S_n} = [\operatorname{soc} G_2]_{S_n}$.

Now let $G \in M_2$. Then G is a classical almost simple group, so $\operatorname{soc} G$ is a classical simple group. G is permutation isomorphic to an action of a classical almost simple group on subspaces, and $\operatorname{soc} G$ is a subgroup of G, so $\operatorname{soc} G$ is also permutation isomorphic to an action on subspaces. Although $\operatorname{soc} G$ is not necessarily primitive, it is a non-trivial normal subgroup of primitive group and is therefore transitive. Thus $[\operatorname{soc} G]_{S_n} \in \mathcal{T}_{cl}$.

Finally we show that f is injective. Let $G_1, G_2 \in M_2$ and suppose that $[\operatorname{soc} G_1]_{S_n} = [\operatorname{soc} G_2]_{S_n}$. Then $\operatorname{soc} G_1 = g^{-1}\operatorname{soc} G_2 g$ for some $g \in S_n$. Therefore

$N_{S_n}(\operatorname{soc} G_1) = N_{S_n}(g^{-1}\operatorname{soc} G_2 g) = g^{-1}(N_{S_n}(\operatorname{soc} G_2))g$. Since $G_i \neq A_n$, by Lemma 7.3.1 we have that $G_1 = N_{S_n}(\operatorname{soc} G_1)$ and $G_2 = N_{S_n}(\operatorname{soc} G_2)$. So $G_1 = g^{-1}G_2 g$, and $[G_1]_{S_n} = [G_2]_{S_n}$.

Thus $f : \mathcal{M}_2 \to \mathcal{T}_{cl}$ is injective, and so $|\mathcal{M}_2| \leq |\mathcal{T}_{cl}|$. □

Lemma 7.3.3. *If $n \neq 6$ then up to (abstract group) isomorphism there are at most*

$$6(n-1)\log_2 n$$

classical simple groups which act transitively with degree n.

Proof. There are six types of classical simple group. A classical simple group of a particular type is determined (up to isomorphism) by its Lie rank, and the order of the field over which its associated vector space is defined. Let T be a classical simple group of Lie rank r, with associated vector space defined over a field of order q, which acts transitively with degree n. Then since $n \neq 6$, by Lemma 2.1.9 we have that $q^r \leq n$. Therefore $2 \leq q \leq n$, and $1 \leq r \leq \log_2 n$. So T may be one of up to six types, there are up to $n-1$ possibilities for q, and up to $\log_2 n$ possibilities for r. Thus there are at most

$$6(n-1)\log_2 n$$

possibilities for T (up to isomorphism). □

Lemma 7.3.4. *The number of actions of degree n of a classical simple group, that are induced by a subspace action of an almost simple group of which it is the socle, is bounded above by*

$$6(\log_2 n + 1).$$

Proof. Let $T(d,q)$ be a classical simple group, where d and q are the dimension and field order respectively of the associated vector space. We fix q and d and consider the different types of classical simple group in turn. For each type we consider the actions of $T(d,q)$ that might be induced by subspace actions of an almost simple group with socle $T(d,q)$, under the various parts of the definition of a subspace action (see page 83). The bounds determined below are not tight, but further refinement is not necessary for our purposes.

First let $T(d,q)$ be linear. Then $T(d,q) = PSL(d,q)$ acts transitively on the set of k-dimensional subspaces for each $1 \leq k \leq d-1$, and there are less than d relevant actions (of any degree) under part (1) of the definition. Furthermore, for each $1 \leq k \leq d/2$, the action of $T(d,q) = PSL(d,q)$ on each of the sets $\{(U,W) : \dim U = k, \dim W = n-k, U \leq W\}$ and $\{(U,W) : \dim U = k, \dim W = n-k, U \cap W = \emptyset\}$ is transitive, so there are certainly less than $2d$ actions under part (2) of the definition.

Now let $T(d,q)$ be symplectic. For each fixed dimension $1 \leq k \leq d-1$, the action of $T(d,q) = PSp(d,q)$ on the set of totally singular k-dimensional subspaces and on the set of non-degenerate k-dimensional subspaces is transitive (some of these sets may be empty - for example the 1-dimensional subspaces are all totally singular, so there are no non-degenerate 1-dimensional subspaces). Therefore there are less than $2d$ actions under part (1) of the definition. If there is a degree n subspace action of $T(d,q) = PSp(d,q)$ under part (3) of the definition, then

$$n = \frac{|Sp(d,q)|}{|O^{\pm}(d,q)|} = \frac{q^{d/2}(q^{d/2}+1)}{2} \text{ or } \frac{q^{d/2}(q^{d/2}-1)}{2}.$$

At most one of these can be true for fixed q and d, so we need consider only one of $O^+(d,q)$ and $O^-(d,q)$. Therefore there is at most one action of $T(d,q)$ under part (3) of the definition.

Finally let $T(d,q)$ be unitary or orthogonal. For each fixed dimension $1 \leq k \leq d-1$, the action of $T(d,q)$ on the set of totally singular k-dimensional subspaces and on the set of non-degenerate k-dimensional subspaces is transitive (again some of these may be empty). Also, when q is even, the action of an orthogonal group on non-singular 1-dimensional subspaces is transitive.

Altogether there are less than $2d$ actions under part (1) of the definition. The action of an orthogonal group under part (3) of the definition of subspace action has already been counted in the symplectic case above.

In all cases there are less than $3d$ relevant actions of $T(d, q)$. Suppose that r is the rank of $T(d, q)$. In our previous proof we observed that $2 \leq q \leq n$, and $1 \leq r \leq \log_2 n$. Since $d \leq 2r + 2$ by Table 2.1.5, we have that $d \leq 2\log_2 n + 2$. Our result follows. $\square$

Lemma 7.3.5. *We have that*

$$|\mathcal{M}_2| < 150n \ln^2 n.$$

Proof. We prove that $150n \ln^2 n$ is an upper bound for $|\mathcal{T}_{cl}|$. Our result then follows by Lemma 7.3.2. First, note that S_6 has one conjugacy class of primitive maximal subgroups (this is the class of subgroups $PGL(2, 5)$ which are isomorphic, but not permutation isomorphic, to S_5.)

Now let $n \neq 6$. Let $[T]_{S_n} \in \mathcal{T}_{cl}$. Then by Lemma 7.3.3, there are at most $6(n-1)\log_2 n$ possible choices for T (up to isomorphism). For a fixed T, the action of T (on Ω) is induced by a subspace action of the almost simple group of which T is the socle. By Lemma 7.3.4 there are at most $6(\log_2 n + 1)$ such actions of T, and so certainly less than this many non-equivalent such actions. Then by Lemma 2.1.2 the number of conjugacy classes of transitive subgroups of S_n which are permutation isomorphic to T is bounded above by $6(\log_2 n + 1)$. Thus

$$\begin{aligned} |\mathcal{T}_{cl}| &\leq 6(n-1)\log_2 n \times 6(\log_2 n + 1) \\ &= 36(n-1)\log_2 n(\log_2 n + 1) \\ &< 150n \ln^2 n. \end{aligned}$$

$\square$

7.4 Type 3 primitive maximal subgroups

We define

$$\begin{aligned} T_{small} &= \{T : T \leq S_n,\, T \text{ simple transitive},\, |T| \leq n^5\}, \text{ and} \\ \mathcal{T}_{small} &= \{[T]_{S_n} : T \in T_{small}\}. \end{aligned}$$

Lemma 7.4.1. *We have that*

$$|\mathcal{M}_3| \leq |\mathcal{T}_{small}|.$$

Proof. Let f be the map $f : \mathcal{M}_3 \to \mathcal{T}_{small}$ defined by

$$f : [M]_{S_n} \mapsto [\mathrm{soc}\,(M)]_{S_n} \qquad M \in M_3.$$

The map is well defined and injective by the same arguments as in the proof of Lemma 7.3.2. Now let $M \in M_3$. Since $|M| \leq n^5$, we have that $|\mathrm{soc}\, M| \leq n^5$, and so $[\mathrm{soc}\, M]_{S_n} \in \mathcal{T}_{small}$. Thus $f : \mathcal{M}_3 \to \mathcal{T}_{small}$ is injective, and so $|\mathcal{M}_3| \leq |\mathcal{T}_{small}|$. □

Lemma 7.4.2. *Up to isomorphism, there are at most $2n^4$ simple groups of order at most n^5, which act transitively with degree n*

Proof. If a simple group acts transitively with degree n it must have an index n subgroup, and hence must have order divisible by n. So there are at most n^4 possible orders for a simple group of order at most n^5 which acts transitively with degree n. By Theorem 2.1.6 there are at most two simple groups of a given order (up to isomorphism). Thus there are at most $2n^4$ abstract simple groups of order at most n^5, which act transitively with degree n. □

Lemma 7.4.3. *The number of conjugacy classes of core-free index n subgroups of a group of order at most n^5 is at most*

$$n^{20 \log_2 n}.$$

Proof. A conjugacy class of subgroups is non-empty, so the number of conjugacy classes of subgroups of a group is at most the number of subgroups. Also, by Lemma 2.2.5, a group of order at most n^5 has at most

$$n^{5(\log_2 n^5 - \log_2 n)} = n^{20 \log_2 n}$$

index n subgroups. We get the following sequence of inequalities.

$$\begin{aligned} |\{[H]_T : H \leq T,\ H \text{ core-free index } n\}| &\leq |\{H : H \leq T,\ H \text{ core-free index } n\}| \\ &\leq |\{H : H \leq T,\ H \text{ index } n\}| \\ &\leq n^{20 \log_2 n}. \end{aligned}$$

□

Lemma 7.4.4. *We have that*

$$|\mathcal{M}_3| \leq 2n^{4(5 \log_2 n + 1)}.$$

Proof. We prove that $2n^{4(5 \log_2 n+1)}$ is an upper bound for $|\mathcal{T}_{small}|$. Our result then follows by Lemma 7.4.1.

Let $[T]_{S_n} \in \mathcal{T}_{small}$. Then by Lemma 7.4.2 there are at most $2n^4$ possible choices for T (up to isomorphism). By Lemma 2.1.2, the number of conjugacy classes of transitive subgroups of S_n which are isomorphic to T is at most the number of conjugacy classes of core-free index n subgroups of T. By Lemma 7.4.3 this is bounded above by $n^{20 \log_2 n}$. Thus

$$|\mathcal{T}_{small}| \leq 2n^4 \times n^{20 \log_2 n} = 2n^{4(5 \log_2 n+1)}.$$

□

7.5 Summary

The table below summarises the main results of this chapter.

Type of maximal subgroup of S_n	Upper bound for $\lvert\mathcal{M}_i\rvert$
1 - symmetric almost simple primitive	n^2
2 - classical almost simple primitive	$150n\ln^2 n.$
3 - small almost simple primitive	$2n^{4(5\log_2 n+1)}$
4 - wreath product primitive	$\log_2 n$
5 - affine primitive	1

Table 7.1: Upper bounds for the number of conjugacy classes of primitive maximal subgroups of S_n of fixed types

Chapter 8

Proof for S_n using the probabilistic method

In Chapter 4 we gave an overview of our proof of Theorem 1.1.1 part 1 for $n \geq 21$ *using the probabilistic method, in order to motivate the work in Chapters 5, 6 and 7. In this chapter we give the full proof.*

8.1 Introduction

We use the strategy presented in Section 4.1. Let n be an odd integer such that $n \geq 21$. Let

$$I = \{\Delta \subset \Omega : |\Delta| < n/2\}.$$

Since n is odd, $|I| = 2^{n-1}$. For a subset $\Delta \subset \Omega$, define

$$C(\Delta) = \{g \in S_n : g \text{ is a } (|\Delta|, n - |\Delta|)\text{-cycle such that } \Delta g = \Delta\}.$$

Now for each $\Delta \in I$, choose $g_\Delta \in C(\Delta)$ uniformly and independently at random. Then define

$$X = \{g_\Delta : \Delta \in I\}.$$

Since $|X| = |I|$, we have $|X| = 2^{n-1}$.

Define a graph $\Gamma = (V, E)$ as follows. The vertices of Γ are the two element subsets of I. We join a pair v, v' of vertices by an edge precisely when $v \cap v' \neq \emptyset$.

Therefore

$$|V| = \binom{|I|}{2} = 2^{n-1}(2^{n-1}-1)/2 = 2^{n-2}(2^{n-1}-1),$$

and each vertex has valency d, where

$$d = 2(|I|-2) = 2(2^{n-1}-2) = 2^n - 4.$$

Now we fix a distinct pair Δ_1, Δ_2 of elements of I, and thus fix the corresponding vertex $\{\Delta_1, \Delta_2\}$ of the graph Γ. We write $E_{\{\Delta_1,\Delta_2\}}$ for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of S_n. We define $p = 1/e2^n$ so we have $ep(d+1) < 1$, and we will prove that

$$Pr(E_{\{\Delta_1,\Delta_2\}}) < p,$$

or if it is more convenient we will prove directly that

$$e(d+1)\, Pr(E_{\{\Delta_1,\Delta_2\}}) < 1.$$

Then we will apply the Lovász Local lemma (Lemma 4.3.1) to conclude that there exists a set of 2^{n-1} elements that generate S_n pairwise.

Define E_{imprim} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup of S_n, and E_{prim} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a primitive maximal subgroup of S_n other than A_n. We have chosen X in such a way that it contains at most one even element (an n-cycle), and at most one element from each of the intransitive maximal subgroups. Therefore if the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of S_n, that subgroup must be transitive, but not A_n. Thus

$$E_{\{\Delta_1,\Delta_2\}} = E_{imprim} \cup E_{prim},$$

and consequently

$$Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim}).$$

8.2 Large values of n

Recall that we defined *large* values of n to be those greater than or equal to 225. In this section we consider these large values of n. First we deal with $Pr(E_{imprim})$. Define E_{imprim_1} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup of S_n which is permutation isomorphic to $S_{n/3} \wr S_3$, and E_{imprim_2} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup of S_n which is permutation isomorphic to $S_{n/k} \wr S_k$, where k is a proper divisor of n such that $k \geq 5$.

Since n is odd, 2 and 4 are not proper divisors of n, so

$$E_{imprim} = E_{imprim_1} \cup E_{imprim_2},$$

and consequently

$$Pr(E_{imprim}) \leq Pr(E_{imprim_1}) + Pr(E_{imprim_2}).$$

Lemma 8.2.1. *If $n \geq 149$, then $Pr(E_{imprim_1}) < p/7$.*

Proof. First we show that if $x \in \mathbb{R}$ and $x \geq 148$, then

$$21e^{11}x^4 2^{-\frac{x}{3}} < 1.$$

We let $F(x)$ be the natural logarithm of $21e^{11}x^4 2^{-\frac{x}{3}}$. Then it suffices to show that $F(x) < 0$.

$$F(x) = \ln 21 + 11 + 4\ln x - x(\ln 2)/3$$
$$\text{and } F'(x) = 4/x - \ln 2/3.$$

Now $\ln 2/3 > 4/x$ when $x > 12/\ln 2 = 17.3$ (to 1 decimal place). So $F'(x)$ is negative if $x \geq 18$. Furthermore $F(148) = -0.2$ (to 1 decimal place). This is the smallest integer value of x for which $F(x) < 0$. Therefore if $x \geq 148$, then $F(x) < 0$, and we have proved our first inequality.

Now by Lemma 6.4.1, we have that $Pr(E_{imprim_1}) < 3e^{10}n^4 2^{-\frac{4n}{3}}$, and so

$$7Pr(E_{imprim_1})/p < 7 \times 3e^{10}n^4 2^{-\frac{4n}{3}} \times e2^n$$
$$= 21e^{11}n^4 2^{-\frac{n}{3}}.$$

Using our first inequality, if $n \geq 148$ then $7Pr(E_{imprim_1})/p < 1$, and our result follows. □

We combine the results from Lemmas 5.2.3 and 5.2.4 to give the following, which we then use for the remaining proofs in this section.

Lemma 8.2.2. *Let n be a positive integer, and let X be S_n or A_n. Let $\mathcal{M}$ be a set of conjugacy classes of subgroups of X. If M is an upper bound for $|\mathcal{M}|$, and m is an upper bound for the order of all the groups in all the conjugacy classes in $\mathcal{M}$, then*

$$Pr(\{g_{\Delta_1}, g_{\Delta_2}\} \subset H \text{ for some } H \in [M]_X \text{ for some } [M]_X \in \mathcal{M})$$

$$\leq \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} m\mathsf{M}.$$

Lemma 8.2.3. *If $n \geq 225$, then $Pr(E_{imprim_2}) < p/7$.*

Proof. First we show that if $x \in \mathbb{R}$ and $x \geq 225$ then

$$\frac{5^3 7}{2^2} e^5 x^{\frac{11}{2}} (x-3) \left(\frac{4x}{5(x-3)}\right)^x < 1.$$

If $x \geq 148$, then $\frac{4x}{5(x-3)} \leq \frac{4 \times 148}{5 \times 145} = \frac{592}{725}$, so

$$\frac{5^3 7}{2^2} e^5 x^{\frac{11}{2}} (x-3) \left(\frac{4x}{5(x-3)}\right)^x < \frac{5^3 7}{2^2} e^5 x^{\frac{13}{2}} \left(\frac{592}{725}\right)^x.$$

We let $F(x)$ be the natural logarithm of the right hand side of this inequality. Then it suffices to show that $F(x) < 0$.

$$F(x) = 5 + \ln \frac{5^3 7}{2^2} + \frac{13}{2} \ln x - x \ln \frac{725}{592}$$
$$\text{and } F'(x) = \frac{13}{2x} - \ln \frac{725}{592}.$$

Now $\frac{13}{2x} < \ln \frac{725}{592}$ when $x > \frac{13}{2} / \ln \frac{725}{592} = 32.1$ (to 1 decimal place). So $F'(x)$ is negative if $x \geq 33$. Furthermore $F(225) = -0.01$ (to 2 decimal places). This is the smallest integer value of x for which $F(x) < 0$. Therefore if $x \geq 225$, then $F(x) < 0$, and we have proved our first inequality.

Let $n > 146$. Then we have an upper bound $e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}}$ for the order of $S_{n/k} \wr S_k$ where $k \geq 5$ from Lemma 2.2.3. The number of conjugacy classes of imprimitive maximal subgroup is the number of proper divisors of n, which is less than $n/2$. Thus we apply Lemma 8.2.2 with these values for m and M respectively.

$$Pr(E_{imprim_2}) < \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}} \times \frac{n}{2}$$

and so

$$\begin{aligned} 7Pr(E_{imprim_2})/p &< 7 \times \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}} \times \frac{n}{2} \times e2^n \\ &= \frac{5^3 7}{2^2} e^5 n^{\frac{11}{2}} (n-3) \left(\frac{4n}{5(n-3)}\right)^n. \end{aligned}$$

Using our first inequality, if $n \geq 225$ then $7Pr(E_{imprim_2})/p < 1$, and our result follows. □

Now we deal with E_{prim}. Maróti tells us that if a primitive group acts with degree $n \geq 25$, then it has order at most 2^{n-1} [17, Corollary 1.4], so for conjugacy classes of primitive maximal subgroups, we apply Lemma 8.2.2 with $m = 2^{n-1}$. Our work in Chapter 7 provides us with an upper bound for the number of conjugacy classes of primitive maximal subgroups. Recall that for odd values of n we used Theorem 7.1.2 to divide primitive maximal subgroups of S_n into five types. For $i \in \{1, \ldots, 5\}$, define E_{prim_i} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a type i primitive maximal subgroup of S_n. Then since n is odd,

$$E_{prim} = E_{prim_1} \cup \ldots \cup E_{prim_5},$$

and consequently

$$Pr(E_{prim}) \leq Pr(E_{prim_1}) + \ldots + Pr(E_{prim_5}).$$

Lemma 8.2.4. *If $n \geq 63$, and $i \in \{1, 2, 4, 5\}$ then $Pr(E_{prim_i}) < p/7$.*

Proof. First we show that if $x \in \mathbb{R}$ and $x \geq 43$, then

$$\frac{525}{e^2}\left(\frac{8e}{x-3}\right)^x x^5 \ln^2 x < 1.$$

We let $F(x)$ be the natural logarithm of the left hand side. Then it suffices to show that $F(x) < 0$.

$$F(x) = \ln 525 - 2 + x[\ln 8 + 1 - \ln(x-3)] + 5\ln x + 2\ln(\ln x),$$
$$\text{and } F'(x) = \ln 8 + 1 - \ln(x-3) - \frac{x}{x-3} + \frac{5}{x} + \frac{2}{x \ln x}.$$

Now $F'(x)$ is a decreasing function if $x \geq 6$, and $F'(13) < 0$, so $F'(x) < 0$ for all $x \geq 13$. Since $F(43) = -0.5$ (to 1 decimal place), if $x \geq 43$ then $F(x) < 0$.

For $i \in \{1, 2, 4, 5\}$, we see from Table 7.1 that the number of conjugacy classes of type i primitive maximal subgroups is bounded above by $150n^2 \ln^2 n$. We apply Lemma 8.2.2 with $m = 2^{n-1}$ and $\mathsf{M} = 300n^2 \ln^2 n$ (we use a higher bound than necessary so that we can apply this proof again for Lemma 9.5.4). We show that if $n \geq 43$, then $7Pr(E_{prim_i})/p < 1$.

$$Pr(E_{prim_i}) < \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times 2^{n-1} \times 300n^2 \ln^2 n,$$

and so

$$\begin{aligned} 7Pr(E_{prim_i})/p &< 7 \times \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times 2^{n-1} \times 300n^2 \ln^2 n \times e2^n \\ &= \frac{525}{e^2} n^5 \ln^2 n \left(\frac{8e}{n-3}\right)^n. \end{aligned}$$

Using our first inequality, if $n \geq 43$ then $7Pr(E_{prim_i})/p < 1$, and our result follows. □

Lemma 8.2.5. *If $n \geq 521$, then $Pr(E_{prim_3}) < p/7$.*

Proof. First we show that if $x \in \mathbb{R}$ and $x \geq 521$, then

$$\frac{56}{e}x^9\left(\frac{4e}{x-3}\right)^{x-1}x^{20\ln x/\ln 2} < 1.$$

We let $F(x)$ be the natural logarithm of the left hand side. Then it suffices to show that $F(x) < 0$. We have

$$\begin{aligned} F(x) &= \ln 56 - 1 + 9\ln x + (x-1)\ln 4e \\ &\qquad\qquad - (x-1)\ln(x-3) + 20\ln^2 x/\ln^2 2, \\ F'(x) &= \frac{9}{x} + \ln 4 + 1 - \frac{x-1}{x-3} - \ln(x-3) + 40\ln x/x\ln^2 2. \end{aligned}$$

Now $40\ln 521/521\ln^2 2 < 1$, so $40\ln x/x\ln^2 2 < 1$ when $x \geq 521$. So

$$F'(x) \leq \ln 4 + 3 - \ln(x-3).$$

Furthermore $\ln 4 + 3 - \ln(521-3) < 0$, so $F'(x) < 0$ for all $n \geq 521$. Finally $F(521) = -320.7$ (to 1 decimal place). Therefore if $x \geq 521$ then $F(x) < 0$.

Now we use our upper bound from Lemma 7.4.4 and apply Lemma 8.2.2 with $m = n^5$ and $\mathsf{M} = 4n^{4(5\log_2 n+1)}$ (here a bound of $\mathsf{M} = 2n^{4(5\log_2 n+1)}$ would suffice, but we use twice this number to allow this proof to apply again later in Lemma 9.5.4, for the A_n case).

$$Pr(E_{prim_3}) < \left(\frac{n}{e}\right)^2\left(\frac{2e}{n-3}\right)^{n-1} \times n^5 \times 4n^{4(5\log_2 n+1)},$$

and so

$$\begin{aligned} 7Pr(E_{prim_3})/p &< 7 \times \left(\frac{n}{e}\right)^2\left(\frac{2e}{n-3}\right)^{n-1} \times n^5 \times 4n^{4(5\log_2 n+1)} \times e2^n \\ &= \frac{56}{e}n^9\left(\frac{4e}{n-3}\right)^{n-1}n^{20\ln n/\ln 2}. \end{aligned}$$

Using our first inequality, if $n \geq 521$ then $7Pr(E_{prim_3})/p < 1$, and our result follows. □

At this point we have sufficient information to conclude that if $n \geq 521$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$. For each degree $n \leq 1000$, Dixon and Mortimer give details of cohorts of primitive groups in their book [7]. The next lemma allows us to use that information to deal with the remaining large odd values of n.

Lemma 8.2.6. *The number of conjugacy classes of primitive maximal subgroups of S_n other than A_n is bounded above by the number of cohorts of primitive groups of degree n.*

Proof. Let $[M]_{S_n}$ be a conjugacy class of primitive maximal subgroups of S_n where $M \neq A_n$. If $\operatorname{soc} M$ denotes the socle of M, then $[\operatorname{soc} M]_{S_n}$ is a corresponding conjugacy class of subgroups, which is represented by exactly one cohort, of degree n. Moreover, by maximality of M, we know that $M = N_{S_n}(\operatorname{soc} M)$, and therefore $[M]_{S_n}$ is the only conjugacy class of primitive maximal subgroups which is represented by this cohort. Thus we have established an injection from the set of conjugacy classes of primitive maximal subgroups of S_n into the set of cohorts of primitive groups of degree n. □

For $n \leq 1000$, we see in [7, Table B.4] that there are at most 10 cohorts of primitive groups which act with degree n, excluding the alternating and affine group. Thus accounting for a possible conjugacy class of affine maximal subgroups (which are present when n is a power of an odd prime), we may apply Lemma 8.2.2 with $\mathsf{M} = 11$.

Lemma 8.2.7. *If $33 \leq n \leq 1000$, then $Pr(E_{prim}) < 5p/7$.*

Proof. First we show that if $x \in \mathbb{R}$ and $33 \leq x \leq 1000$, then

$$\frac{154}{5e} x^2 \left(\frac{8e}{30}\right)^{x-1} < 1.$$

We let $F(x)$ be the natural logarithm of the right hand side. Then it suffices to show that $F(x) < 0$.

$$\begin{aligned} F(x) &= \ln \frac{308}{5} - 1 + 2 \ln x - (x-1) \ln \frac{30}{8e} \\ \text{and } F'(x) &= \frac{2}{x} - \ln \frac{30}{8e}. \end{aligned}$$

Now $\frac{2}{x} < \ln \frac{30}{8e}$ when $x > 2 / \ln \frac{30}{8e} = 6.2$ (to 1 decimal place). So $F'(x)$ is negative for $x \geq 7$. Furthermore $F(33) = -0.2$ (to 1 decimal place). Therefore if $x \geq 33$ then $F(x) < 0$.

Now we apply Lemma 8.2.2 with $m = 2^{n-1}$. We use $\mathsf{M} = 22$ so that this proof can be used again later for Lemma 9.5.6, although $\mathsf{M} = 11$ would suffice here.

$$Pr(E_{prim}) < \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times 2^{n-1} \times 22,$$

and so

$$\begin{aligned} 7Pr(E_{prim})/5p &< 7 \times \left(\frac{n}{e}\right)^2 \left(\frac{2e}{n-3}\right)^{n-1} \times 2^{n-1} \times 22 \times \frac{e2^n}{5} \\ &= \frac{308}{5e} n^2 \left(\frac{8e}{n-3}\right)^{n-1} \end{aligned}$$

If $n \geq 33$, then $n - 3 \geq 30$ and so

$$7Pr(E_{prim})/5p < \frac{308}{5e} n^2 \left(\frac{8e}{30}\right)^{n-1}.$$

Using our first inequality, if $33 \leq n \leq 1000$ then $7Pr(E_{prim})/5p < 1$, and our result follows. □

We are now in a position to give a proof of part of our main result. First we summarise the results so far from this section. Recall that n is odd.

If ...	then ...
$n \geq 149$	$Pr(E_{imprim_1}) < p/7$
$n \geq 225$	$Pr(E_{imprim_2}) < p/7$
$n \geq 43$	$Pr(E_{prim_i}) < p/7$ for $i \in \{1, 2, 4, 5\}$
$n \geq 521$	$Pr(E_{prim_3}) < p/7$
$33 \leq n \leq 1000$	$Pr(E_{prim}) < 5p/7$

Table 8.1: Summary of results in Section 8.2

Proof of Theorem 1.1.1 part 1 for $n \geq 225$. As remarked earlier,

$$Pr(E_{imprim}) \leq Pr(E_{imprim_1}) + Pr(E_{imprim_2}),$$

$$Pr(E_{prim}) \leq Pr(E_{prim_1}) + \ldots + Pr(E_{prim_5}),$$

and

$$Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim}).$$

Using the results given in the table above, we conclude that if $n \geq 225$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$. Our result follows. □

8.3 Medium values of n

Recall that we defined *medium* values of n to be those such that $33 \leq n \leq 223$. By Lemma 8.2.7, if $33 \leq n \leq 1000$, then $Pr(E_{prim}) < 5p/7$. Therefore for medium values of n, it remains to show that $Pr(E_{imprim}) < 2p/7$.

Lemma 8.3.1. *If* $3 \leq n \leq 223$ *and if* $n \notin \{5, 9, 15, 21, 27\}$*, then we have*

$$Pr(E_{imprim}) < 2p/7.$$

Proof. This proof uses two `GAP` programs and applies the theory on imprimitive maximal subgroups of S_n developed in Chapter 6.

The first program, with filename `countingpartitions` and included as Appendix B, creates two functions, `p(x,y)` and `op(x,y)`. The variable `x` must be a positive integer, and the variable `y` must be either a positive integer, or a list of integers which sum to `x`. Then the `GAP` functions `p(x,y)` and `op(x,y)` are the same functions as in Lemmas 6.5.1 and 6.5.3, so if `x`$= 0$ then `p(x,y)` and `op(x,y)` both return the value 1. If `x`> 0, if `y` is an integer, then `p(x,y)` returns the number of partitions of a set of order `x` into subsets of order `y`, and if `y` is a list, then `p(x,y)` returns the number of partitions of a set of order `x` into subsets of the orders in the list `y`. The function `op(x,y)` is the equivalent for ordered partitions.

The second program, with filename `medium` and included as Appendix C, uses these two functions. As remarked in Chapter 6, we have that

$$Pr(E_{imprim}) \leq \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{\substack{k|n \\ k\neq 1,n}} \sum_{H\in\mathcal{H}_k} |C(\Delta_1) \cap H||C(\Delta_2) \cap H|.$$

Our work in Section 6.5 give us an upper bound for $|C(\Delta_1) \cap H||C(\Delta_2) \cap H|$ as a function of d_1, d_2, i, k and n, where $d_1 = |\Delta_1|$, $d_2 = |\Delta_2|$, and $i = |\Delta_1 \cap \Delta_2|$, so using the inequality above, we have an upper bound for $Pr(E_{imprim})$ as a function of d_1, d_2, i and n. For each n there are many different possible combinations of d_1, d_2, i, each of which will give a different upper bound for $Pr(E_{imprim})$.

Before we run the program `medium`, we must define a variable `test`, which must be a list of integers containing the values of n which we wish to consider. For each odd integer in `test`, our program loops through each possible combination of d_1, d_2, and i in turn. We now explain these combinations. The variables `d1`, `d2` and `i` represent d_1, d_2, and i respectively. Recall that $0 \leq d_1, d_2 \leq (n-1)/2$, and at most one of $d_1, d_2 = 0$. We consider `d1` as each integer in the list `[1..(n-1)/2]`. For each `d1` we consider each integer `d2` in the list `[0..d1]`. We consider only `d2`$\leq$`d1`, because our upper bound for $Pr(E_{imprim})$ is symmetric in the variables `d1` and `d2`, that is, the value is unaffected if we exchange these two variables. This reduces computer processing time. Also, we do not consider the case `d1`$= 0$ because at most one of `d1` and `d2` is zero. The order of the intersection `i` can be anything from zero to $d_1 - 1$ if $d_1 = d_2$, or zero to $\min(d_1, d_2)$ otherwise. All of these values are considered.

For each possible combination of `d1`, `d2` and `i`, we assign to a variable `combprob` the calculated upper bound for $Pr(E_{imprim})$ for this particular combination. We append `combprob` to a variable list called `imprimprob`. After all possible combinations, we let the variable `ub` be the maximum of the list `imprimprob`, so `ub` is an upper bound for $Pr(E_{imprim})$ for this value of n. If `ub`$< 2p/7$ then we know that $Pr(E_{imprim}) < 2p/7$. Otherwise we have failed to prove that $Pr(E_{imprim})$ is sufficiently small, and this value of n is added to the list `bad_n`.

This proof therefore is acheived by the following sequence of commands and output in `GAP`:

```
gap>Read("c:/gap4r4/countpartitions");
gap>test:=[3..224];
>[3..224]
gap>Read("c:/gap4r4/medium");
gap>bad_n;
>[5,9,15,21,27]
```

□

Proof of Theorem 1.1.1 part 1 for $33 \leq n \leq 223$. By Lemmas 8.2.7 and 8.3.1, we have that if $33 \leq n \leq 223$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$. Our result follows. □

8.4 Small values of n

Our result does not follow for values of n less than 33 because the bound for $Pr(E_{prim})$ is too high. In the next lemma, for the small values of n, we use the `GAP` data library to provide the orders of the primitive maximal subgroups of S_n, and thus obtain a tighter upper bound for $Pr(E_{prim})$.

Lemma 8.4.1. *If* $23 \leq n \leq 31$*, then* $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$.

Proof. This proof uses two `GAP` programs. The first is called `countpartitions`, and was used and discussed in the proof of Lemma 8.3.1. The second is called `small` and is included as Appendix D. Before running the program `small`, we must define a variable called `test`, which must be a list of integers containing the values of n which we wish to consider. The first part of `small` is identical to the first part of program `medium` which was used in Lemma 8.3.1, and it calculates an upper bound for $Pr(E_{imprim})$ using the theory developed in Chapter 6. This bound is assigned to the variable `ub_imprim`.

The second part of `small` calculates an upper bound for $Pr(E_{prim})$. Let $M_1, \ldots, M_r$ be a complete set of representatives of the conjugacy classes of primitive maximal subgroups of S_n other than A_n. Then by Lemmas 5.2.2

and 5.2.4,

$$Pr(E_{prim}) < \sum_{i=1}^{r} \frac{n^2|M_i|}{\frac{(n-1)}{2}!\frac{(n-3)}{2}!}.$$

The GAP command `MaximalSubgroupClassReps` speedily provides candidates for the M_i for the small values of n under consideration. The program `small` calculates the upper bound for $Pr(E_{prim})$ given in this inequality, and assigns it to the variable `ub_prim`.

Recall that $Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim})$, and we aim to show that $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$ where $p = 1/e2^n$. We have an upper bound `ub_imprim+ub_prim` for $Pr(E_{\{\Delta_1,\Delta_2\}})$, and in the final part of `small` we compare this bound to p. If it exceeds p, that is, if our bound fails to be sufficiently low, we add the value of n under consideration to the list `bad_n`.

This proof therefore is completed by the following sequence of commands and output in GAP:

```
gap>Read("c:/gap4r4/countpartitions");
gap>test:=[5..31];
>[5..31]
gap>Read("c:/gap4r4/small");
gap>bad_n;
>[5,7,9,11,13,15,17,19,21].
```

□

8.5 $n = 21$

The bound for $Pr(E_{prim})$ obtained in the previous proof is too high to be used in the case $n = 21$, so in Lemma 8.5.2 we calculate an even lower bound. We also increase our target by reducing the degree of our graph Γ. We give a preliminary lemma. Recall the notation $C(\Delta)$ which denotes the set of elements of S_n which have orbits Δ and $\Omega\backslash\Delta$, and let $\mathcal{P}$ be the conjugacy class of maximal subgroups of S_n which are permutation isomorphic to $P\Gamma L(3,4)$ (acting with degree 21 in the usual way).

Lemma 8.5.1. *S_{21} has three conjugacy classes of primitive maximal subgroups other than A_{21}, including $\mathcal{P}$ as defined above.*

1. *The only primitive maximal subgroups of S_{21} which contain a bi-cycle or a 21-cycle are those in $\mathcal{P}$.*

2. *Let $H \in \mathcal{P}$. Then H contains 48 elements which are $7, 14$-cycles, from each of 360 different $C(\Delta)$. In total H contains $48 \times 360 = 17\,280$ elements which are $7, 14$-cycles. In addition, H contains $11\,520$ elements which are 21-cycles. H contains no other bi-cycles.*

3. *Let $\Delta \subset \Omega$ such that $|\Delta| = 7$. Then $|C(\Delta) \cap H| \neq \emptyset$ for exactly $7!14!/336$ different subgroups $H \in \mathcal{P}$.*

Proof. 1. We use a `GAP` program called `s21bicycles` which is included as Appendix E. First `s21bicycles` puts representatives of the conjugacy classes of primitive maximal subgroups of S_{21} other than A_{21} in a list called `primsubgroups`. Second, it determines the cycle lengths of the elements of each of these representatives, and whenever it encounters a 21-cycle or a bi-cycle, it adds the name of the representative together with the cycle lengths to a set called `bicycles`. This proof is therefore achieved by the following sequence of commands and output in `GAP`:

```
gap>Read("c:/gap4r4/s21subgroups");
gap>primsubgroups;
>[PGL(2,7), S(7), PGammaL(3,4)].
gap>bicycles;
>[[PGammaL(3,4),[21]], [PGammaL(3,4),[7,14]].
```

2. Again we use the `GAP` program called `s21bicycles`. The third part of this program assigns the representative of $\mathcal{P}$ to the variable `pgl`. It makes a list `714cycles` of all the $(7, 14)$-cycles in `pgl`, and a set `7orbits` of the orbits of length 7 of these bi-cycles. It also makes a list of the 21-cycles in `pgl`. Then

for each orbit in `7orbits`, it counts how many of the elements of `714cycles` have this as an orbit, and assigns this total to a set called `results`. This proof is therefore achieved by the following sequence of `GAP` commands and output.

```
gap>Read("c:/gap4r4/s21bicycles");
gap>Length(set7orbits);
>360
gap>results;
>[48].
gap>Length(714cycles);
>17280
gap>Length(21cycles);
>11520
```

3. Let P be a fixed subgroup which is permutation isomorphic to $P\Gamma L(3,4)$ (so $P \in \mathcal{P}$). We count pairs (Δ, H) in two ways, where $\Delta \subset \Omega$ and $|\Delta| = 7$, H is conjugate to P (so $H \in \mathcal{P}$), and $C(\Delta) \cap H \neq \emptyset$. Let r be the number of such pairs.

First we have $r = xy$ where x is the number of $\Delta \subset \Omega$ such that $|\Delta| = 7$, so $x = \binom{21}{7}$. The number which we wish to determine is y, that is the number of subgroups $H \in \mathcal{P}$ such that $C(\Delta) \cap H \neq \emptyset$ for a fixed $\Delta \subset \Omega$ with $|\Delta| = 7$ (this number is the same for all such Δ because all such $C(\Delta)$ are conjugate in S_{21}). Second we have $r = zw$, where z is the number of Δ such that $C(\Delta) \cap H \neq \emptyset$ for a fixed subgroup $H \in \mathcal{P}$ (again this number is the same for such subgroups because all $C(\Delta)$ are conjugate in S_n). By part 2 we have $z = 360$. By the orbit-stabiliser theorem we have $w = |\mathcal{P}| = |S_{21} : N_{S_{21}}(P)|$, and by maximality $N_{S_{21}}(P) = P$. We use `GAP` to provide the order of $P\Gamma L(3,4)$.

```
gap>Order(pgl);
>120,960.
```

So $w = 21!/120\,960$. Equating the two expressions for r gives

$$r = \binom{21}{7} y = 360 \times 21!/120\,960,$$

so $y = 7!14!/336$. □

Even though this result allows us to calculate a tighter upper bound for $P(E_{prim})$, it is not low enough to apply the Lovász Local lemma. We solve this problem in our next lemma. Recall that in Section 8.1 we defined a set I of $2^{n-1} = 2^{21-1}$ subsets of $\Omega = \{1, \ldots, 21\}$, a set X of order 2^{21-1} which we hope will be a pairwise generating set for S_{21}, and a graph Γ which has the two element subsets of I as its vertex set. We need to prove that

$$Pr(E_{\{\Delta_1,\Delta_2\}})\, e(d+1) < 1,$$

where d is the degree of Γ. If $n = 21$, then part 1 of Lemma 8.5.1 tells us that only some of the pairs of elements of X can possibly be contained in a maximal subgroup of S_n. As a result of this, we can reduce the maximum degree of our graph Γ, and then our bound for $Pr(E_{\{\Delta_1,\Delta_2\}})$ is indeed sufficiently low.

Lemma 8.5.2. $\mu(S_{21}) = 2^{21-1}$.

Proof. Let $n = 21$. The set X contains at most one even element (a 21-cycle), and at most one element from each of the intransitive maximal subgroups of S_{21}. By Lemma 6.3.1, the only elements of X which are contained in imprimitive maximal subgroups of S_{21} are the $3, 18$-cycles, the $6, 15$-cycles, the $9, 12$-cycles, the $7, 14$-cycles and the 21-cycle. By our previous lemma, the only elements of X which are contained in primitive maximal subgroups of S_{21} are the $7, 14$-cycles and the 21-cycle. It follows that the pair $g_{\Delta_1}, g_{\Delta_2}$ can only be contained in a maximal subgroup if $\{\Delta_1, \Delta_2\} \subset I'$ where

$$I' = \{\Delta \subset \Omega : |\Delta| \in \{0, 3, 6, 7, 9\}\}.$$

Indeed for any vertex v of Γ, the probability $Pr(E_v)$ is non-zero only when $v \subset I'$. Therefore we may reduce the edge set of Γ so that a pair v, v' of vertices is joined only we have both $v \subset I'$ and $v' \subset I'$ (as well as $v \cap v' \neq \emptyset$). The graph Γ retains the property that for each vertex v, the event E_v is independent of the events $\{E_u : u \neq v\}$. However, since

$$|I'| = \binom{21}{0} + \binom{21}{3} + \binom{21}{6} + \binom{21}{7} + \binom{21}{9} = 465\,805,$$

the maximum degree of Γ is now

$$d = 2(|I'| - 2) = 931\,606.$$

Now using Lemma 8.5.1 we find an upper bound for $Pr(E_{prim})$. We have

$$Pr(E_{prim}) \leq \sum_{H \in \mathcal{P}} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|}.$$

$Pr(E_{prim}) = 0$ unless $|\Delta_1|, |\Delta_2| \in \{0, 7\}$. Let $H \in \mathcal{P}$. At most one of $|\Delta_1|, |\Delta_2|$ is equal to 0, so suppose without loss of generality that $|\Delta_1| = 7$. Then if $C(\Delta_1) \cap H \neq \emptyset$ we have $|C(\Delta_1) \cap H|/|C(\Delta_1)| = 48/6!13!$. If $|\Delta_2| = 7$, then similarly if $C(\Delta_2) \cap H \neq \emptyset$ we have $|C(\Delta_2) \cap H|/|C(\Delta_1)| = 48/6!13!$. If $|\Delta_2| = 0$, then by Lemma 8.5.1 if $C(\Delta_2) \cap H \neq \emptyset$ we have $|C(\Delta_2) \cap H|/|C(\Delta_1)| = 11\,520/20!$. Since $11\,520/20! < 48/6!13!$, we have

$$Pr(E_{prim}) < \frac{7!14!}{336} \times \left(\frac{48}{6!13!}\right)^2 = 112/5!12!.$$

Finally, we use the `GAP` program `countpartitions` as in previous proofs, and then a program called `n21`, which is included as Appendix F. The first part of `n21` is identical to the first part of the programs `medium` and `small` which were used in Lemmas 8.3.1 and 8.4.1 respectively, and calculates an upper bound for $Pr(E_{imprim})$ using the theory developed in Chapter 6. This bound is assigned to the variable `ub_imprim`.

The second part of `n21` calculates an upper bound for $Pr(E_{prim})$ using the inequality above, and assigns it to the variable `ub_prim`. So we have an upper bound `ub=ub_imprim+ub_prim` for $Pr(E_{\{\Delta_1,\Delta_2\}})$. In the final part of `n21` we check that `ub` $e(d+1) < 1$, and if not we add this value of n to the list `bad_n` (of course in this case we have $n = 21$).

We run the following sequence of commands and output in `GAP`:

```
gap>Read("c:/gap4r4/countpartitions"); test:=[21];
>[21]
gap>Read("c:/gap4r4/n21"); bad_n;
>[ ].
```

Therefore `ub` $e(d+1) < 1$, so $e(d+1)\,Pr(E_{\{\Delta_1,\Delta_2\}}) < 1$. We apply the Lovász Local lemma and conclude that the probability that X generates S_{21} pairwise is non-zero. $\square$

Chapter 9

Proof for A_n

Our results for $\mu(S_n)$ concerns odd values of n. In this chapter we prove Theorem 1.1.1 parts 3 and 4, which concern $\mu(A_n)$ where $n \equiv 2 \pmod 4$. We use a probabilistic method to prove that if $n \equiv 2 \pmod 4$ and $n \geq 22$, then $\mu(A_n) = 2^{n-2}$. We give a constructive proof that $\mu(A_6) = 11 < 2^{6-2}$.

9.1 Introduction

$\mu(A_n) = 2^{n-2}$ holds trivially when $n = 2$, since the set $\{e\}$ which contains only the identity permutation, generates $A_2 = \{e\}$ pairwise. Let $n \equiv 2 \pmod 4$ and $n \geq 6$. First we give covering of A_n of order 2^{n-2}. Define collections of subsets of Ω by

$$I_1 = \{\Delta \subset \Omega : |\Delta| \text{ is odd and } |\Delta| < n/2\},$$
$$I_2 = \{\Delta \subset \Omega : |\Delta| = n/2 \text{ and } 1 \in \Delta\},$$
$$I = I_1 \cup I_2.$$

Now for each $\Delta \in I$, define the subgroup M_Δ of A_n to be the maximal subgroup which preserves the partition $\{\Delta, \Omega\backslash\Delta\}$ of Ω. If $\Delta \in I_1$, then M_Δ is intransitive and $M_\Delta \cong (S_{|\Delta|} \times S_{(n-|\Delta|)}) \cap A_n$. If $\Delta \in I_2$, then M_Δ is imprimitive and $M_\Delta \cong (S_{n/2} \wr S_2) \cap A_n$. For all $\Delta \in I$, M_Δ is a maximal subgroup of A_n. Note that $n/2$ is odd because $n \equiv 2 \pmod 4$, and

$$|I| = |I_1| + |I_2| = \binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{n/2-2} + \frac{1}{2}\binom{n}{n/2},$$

so $|I| = 2^{n-2}$ by Lemma 2.2.1. Then $\{M_\Delta : \Delta \in I\}$ is a set of 2^{n-2} subgroups of A_n, and in our first lemma we prove that this is a covering of A_n. (Maróti proves in [18, Theorem 4.1] that this covering is actually a minimal covering).

Lemma 9.1.1. *If n is an even integer such that $n \equiv 2 \pmod 4$ and $n \geq 6$, then $\{M_\Delta : \Delta \in I\}$ is a covering of A_n.*

Proof. Let n be an integer such that $n \equiv 2 \pmod 4$, and let $g \in A_n$. We write g as a product of disjoint cycles $g = g_1 \ldots g_r$. We make the following observations.

1. The sum of the lengths of the orbits of g is n which is even. Therefore an even number of the orbits must be of odd length.

2. A cycle of even length is an odd permutation. Since g is an element of A_n, an even number of the cycles $g_1, \ldots, g_r$ must be odd permutations, thus an even number of the orbits must be of even length.

Therefore r is even (in particular $r \neq 1$ and g is not an n-cycle.)

First suppose all the orbits of g are of even length. Let Δ be a set which contains alternate elements from each of the cycles of g, including the element 1 from the cycle which contains 1. For example if $g = (1\,2)(3\,4\,5\,6) \in A_6$, then we could have $\Delta = \{1, 3, 5\}$. Then $\Delta \in I_2$ and $g \in M_\Delta$.

If g is an $(n/2, n/2)$-cycle (so g has exactly two orbits, both of odd length), then let Δ be the orbit which contains the element 1. Then $\Delta \in I_2$ and $g \in M_\Delta$.

Otherwise g has two or more orbits of odd length, and at least one of these, Δ say, must be of odd length less than $n/2$. Then $\Delta \in I_1$ and $g \in M_\Delta$.

In all cases, $g \in M_\Delta$ for some $\Delta \in I$, so the union of the M_Δ is all of A_n. □

A pairwise generating set contains at most one element from each subgroup in any covering, so a pairwise generating set for A_n contains at most 2^{n-2} elements, so $\mu(A_n) \leq 2^{n-2}$.

Lemma 9.1.2. *If n is an integer such that $n \equiv 2 \pmod 4$ and $n \geq 6$, and if $\mu(A_n) = 2^{n-2}$, then a maximal pairwise generating set consists of 2^{n-2} bicycles which are each a product of two disjoint cycles of odd length.*

Proof. Suppose that $\mu(A_n) = 2^{n-2}$ and X generates A_n pairwise with $|X| = 2^{n-2} = |I|$. Let $g \in X$, so then g must be contained in only one of the subgroups in the covering $\{M_\Delta : \Delta \in I\}$. We write g as a product of disjoint cycles $g = g_1 \ldots g_r$ as in the proof of the previous lemma, and let Δ_i be the orbit of the cycle g_i.

If all of the orbits of g are of even length, then again as in the proof of the previous lemma, let Δ be a set which contains alternate elements from each of the cycles of g, including the element 1 from the cycle which contains 1. Since $r \geq 2$ there are at least two possibilities for Δ. For example if $g = (1\,2)(3\,4\,5\,6) \in A_6$, then $\Delta = \{1, 3, 5\}$ or $\Delta = \{1, 4, 6\}$. Therefore g is contained in more than one M_Δ with $\Delta \in I_2$. Therefore at least two of the orbits must be of odd length.

Suppose g has two or more orbits of odd length and two or more orbits of even length. If there are two orbits, Δ_1, Δ_2 say, of odd length at most $n/2$, then $g \in M_{\Delta_1}$ and $g \in M_{\Delta_2}$. Otherwise there is one orbit Δ_1 say of odd length greater than $n/2$, and the sum of the lengths of the other orbits is less than $n/2$. Suppose that Δ_2 is another orbit of odd length and Δ_3, Δ_4 are orbits of even length. Then $g \in M_{\Delta_2 \cup \Delta_3}$, $g \in M_{\Delta_2 \cup \Delta_4}$, and $\Delta_2 \cup \Delta_3$, $\Delta_2 \cup \Delta_4 \in I_1$. In both of these cases, g is contained in more than one M_Δ. Therefore none of the orbits are of even length.

Therefore all the orbits of g must be of odd length. If $r \geq 4$, then at least two, Δ_1, Δ_2 say, are of length $\leq n/2$. Then $g \in M_{\Delta_1}$ and $g \in M_{\Delta_2}$, that is g

is contained in more than one M_Δ.

Therefore $r = 2$ and g is a product of two disjoint cycles of odd length. □

9.2 $n = 6$

We follow a short diversion to consider this small case. The five conjugacy classes of maximal subgroups of A_6 are determined using `GAP` or the Atlas of Finite Groups [5], and are given in Table 9.1. (The intransitive subgroups A_5

Class		Order	Number of copies
Intransitive	A_5	60	6
Intransitive	$(S_2 \times S_4) \cap A_6$	24	15
Imprimitive	$(S_2 \wr S_3) \cap A_6$	24	15
Imprimitive	$(S_3 \wr S_2) \cap A_6$	36	10
Linear	$\mathrm{PSL}(2,5)$	60	6

Table 9.1: The maximal subgroups of A_6

are isomorphic, but not permutation isomorphic, to the primitive subgroups $\mathrm{PSL}(2,5)$.) There are six possible cycle structures for an element of A_6, these are given in Table 9.2.

The following `GAP` code tells us that the maximal subgroup $\mathrm{PSL}(2,5)$ of A_6

Cycle structure	Example	Number
-	e	1
2,2	(12)(34)	$15 \cdot 3 = 45$
2,4	(12)(3456)	$15 \cdot 3! = 90$
3	(123)	$20 \cdot 2 = 40$
3,3	(123)(456)	$10 \cdot 4 = 40$
5	(12345)	$6 \cdot 4! = 144$
	Total	360

Table 9.2: The cycle structures of the elements of A_6

contains twenty four $(1,5)$-cycles (in two conjugacy classes each of order 12) and twenty $(3,3)$-cycles.

```
gap>mscr:=MaximalSubgroupsClassReps(AlternatingGroup(6));
>m:=mscr[6]; bicycles:=[m];
>for c in ConjugacyClasses(m) do
>   cl:=CycleLengths(Representative(c),[1..6]);
>   if Length(cl)=2 then Add(bicycles, [cl,Length(AsSet(c))]; fi;
>od;
gap>bicycles;
>[PSL(2,5),[[1,5],12],[[1,5],12],[[3,3],20]
```

Lemma 9.2.1. *We have $\mu(A_6) = 11$.*

Proof. First we prove that $\mu(A_6) \leq 11$, and then we give a pairwise generating set for A_6 of order 11.

Let X be a pairwise generating set for A_6 of order $\mu(A_6)$. Then $\mu(A_6) = |X| = x+y+z+v+w$, where x, y, z, w and v are the number of $(2,2)$-cycles, $(2,4)$-cycles, 3-cycles, $(3,3)$-cycles, and 5-cycles respectively in X. Each of the six copies of $\mathrm{PSL}(2,5)$ in A_6 contains twenty $(3,3)$-cycles, and A_6 contains in total $\frac{1}{2}\binom{6}{3} \cdot 4 = 40$ elements which are $(3,3)$-cycles, so a fixed $(3,3)$-cycle must be contained in three copies of $\mathrm{PSL}(2,5)$. Furthermore, a fixed 5-cycle is contained at least one of the six copies of $\mathrm{PSL}(2,5)$, so we have

$$3v + w \leq 6.$$

A 5-cycle is contained in one copy of A_5, a $(2,2)$-cycle is contained in two copies of A_5, and a 3-cycle is contained in three copies of A_5, so we have

$$2x + 3z + w \leq 6.$$

It follows that $x+z+v+w \leq 6$. A fixed $(2,4)$-cycle is contained in two of the ten copies of $S_3 \wr S_2$, so $y \leq 5$. Therefore $\mu(A_6) = |X| = x+y+z+v+w \leq 11$.

Now let X be the set

$$\{(2,3,4,6,5),(1,3,4,6,5),(1,4,6,5,2),(1,6,5,2,3),$$
$$(1,2,3,4,6),(1,5,2,3,4),(1,2)(3,4,5,6),(1,6,5,3)(2,4),$$
$$(1,2,3,5)(4,6),(1,5,2,4)(3,6),(1,3)(2,5,4,6)\}.$$

Using `GAP`, we confirm that this is a pairwise generating set for A_6. We assign the elements of X to a list `x`, and then the following code yields a sequence of integers which are all 4, 5 or 360.

```
gap> for g in x do for h in x do
>       Print(Order(Group(g,h)));
>    od; od;
```

Since $|X| = 11$, our result follows. □

9.3 Probabilistic proof

Recall our definition of I given in Section 9.1. For each $\Delta \in I$, define

$$C(\Delta) = \{g \in S_n : g \text{ is a } (|\Delta|, n - |\Delta|)\text{-cycle such that } \Delta g = \Delta\}.$$

Since n is even, a $(|\Delta|, n - |\Delta|)$-cycle is an even permutation, and each $C(\Delta)$ contains bi-cycles from A_n where the length of each cycle is odd. We choose a set X of elements of A_n by choosing elements $g_\Delta \in C(\Delta)$ uniformly and independently at random. Then define

$$X = \{g_\Delta : \Delta \in I\}.$$

Now define a graph $\Gamma = (V, E)$ as follows. The vertices are the two element subsets of I, and a pair v, v' of vertices are joined by an edge precisely when $v \cap v' \neq \emptyset$. Then the degree of each vertex is

$$d = 2(|I| - 2) = 2(2^{n-2} - 2) = 2^{n-1} - 4.$$

We fix a distinct pair $g_{\Delta_1}, g_{\Delta_2}$ of elements of X, and thus fix the corresponding vertex $\{\Delta_1, \Delta_2\}$ of Γ.

We write $E_{\{\Delta_1,\Delta_2\}}$ for the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of A_n. As in the proof for S_n in Chapter 8, we define $p = 1/e2^n$ so we have $ep(d+1) < 1$, and we will prove that

$$Pr(E_{\{\Delta_1,\Delta_2\}}) < p,$$

or if it is more convenient we will prove directly that

$$e(d+1)\, Pr(E_{\{\Delta_1,\Delta_2\}}) < 1.$$

Then by the Lovász Local lemma (Lemma 4.3.1) we conclude that there exists a set of 2^{n-2} elements that generate A_n pairwise. This definition of p is smaller than necessary, but allows us to use some results from the S_n case.

We have chosen X in such a way that the pair $g_{\Delta_1}, g_{\Delta_2}$ is not contained in an intransitive subgroup of A_n. Therefore

$$E_{\{\Delta_1,\Delta_2\}} = E_{imprim} \cup E_{prim},$$

where E_{imprim} is the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup of A_n, and E_{prim} is the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a primitive maximal subgroup of A_n. Consequently

$$Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim}).$$

9.4 Primitive maximal subgroups of A_n

In Theorem 9.4.1 we show that if $n \equiv 2 \pmod 4$, then a primitive maximal subgroup of A_n is almost simple, and we subdivide this class of maximal subgroups further. Recall the definition of a subspace action of an almost simple group, given on page 83.

Theorem 9.4.1. *Let n be a positive integer such that $n \equiv 2 \pmod 4$, and let M be a primitive maximal subgroup of A_n. Then M is one of the following:*

1. *An almost simple group with socle A_m, for some integer $m \leq n-1$, acting on the set of k-subsets of $\{1, \ldots, m\}$ for some integer k such that $2 \leq k \leq m-1$, or on the set of partitions of $\{1, \ldots, m\}$ into k-subsets, for some proper divisor k of m;*

2. *An almost simple group (with classical socle) acting on subspaces;*

3. *An almost simple group of order at most n^5.*

Proof. If M is almost simple (so M is in class 6 of the O'Nan-Scott theorem), then by Theorem 7.1.1, M is in one of the three parts above.

Suppose that M is in class 5 (diagonal) of the O'Nan-Scott theorem. Then $n = |T|^{k-1}$ where T is a non-abelian finite simple group, and k is an integer such that $k \geq 2$. However, by Corollary 2.1.8, the order of a non-abelian finite simple group is divisible by 4. So n is divisible by 4 which contradicts our hypothesis. So class 5 of the O'Nan-Scott theorem is ruled out.

Suppose that M is in class 4 (affine) of the O'Nan-Scott theorem, then since n is even, it is equal to a non-trivial power of 2. So n is divisible by 4 which contradicts our hypothesis. So class 4 of the O'Nan-Scott theorem is also ruled out.

Suppose that M is in class 3 (wreath) of the O'Nan-Scott theorem, then since n is even, it is equal to a non-trivial power of an even number. So again n is divisible by 4 which contradicts our hypothesis. So class 3 of the O'Nan-Scott theorem is also ruled out.

(Classes 1 and 2 of the O'Nan-Scott theorem do not contain primitive subgroups). □

We now define three sets of maximal subgroups of A_n, and three sets of conjugacy classes of maximal subgroups of A_n. For $i \in \{1, 2, 3\}$ define G_i to be the set of maximal subgroups M of A_n under part i of Theorem 9.4.1 above.

Then define

$$\mathcal{G}_i = \{[M]_{S_n} \mid M \in G_i\},$$

so $\mathcal{G}_i$ is the set of conjugacy classes of subgroups in G_i.

We use the work in Chapter 7, and the fact that a conjugacy class $[G]_{S_n}$ of subgroups of S_n corresponds directly to either one or two conjugacy classes $[G \cap A_n]_{A_n}$ of subgroups of A_n, to provide upper bounds for $|\mathcal{G}_1|$, $|\mathcal{G}_2|$ and $|\mathcal{G}_3|$.

First recall that on page 85 we defined $\mathcal{M}_1$ to be the set of conjugacy classes of maximal subgroups S_m of S_n, where S_m is acting on k-sets. In Lemma 7.2.1 we proved that $|\mathcal{M}_1| \leq n^2$. In fact, that proof did not depend in any way on maximality of the subgroups, so the bound applies equally to the set of conjugacy classes of (not necessarily) maximal subgroups S_m of S_n, where S_m is acting on k-sets. It follows that

$$|\mathcal{G}_1| \leq 2n^2.$$

Now recall that on page 88 we defined $\mathcal{T}_{cl}$ to be the set of conjugacy classes of classical simple subgroups of S_n that are the socles of almost simple groups acting on subspaces, and in Lemma 7.3.5 we proved that $|\mathcal{T}_{cl}| \leq 150n \ln^2 n$. It follows that

$$|\mathcal{G}_2| \leq 300n \ln^2 n.$$

Finally, recall that on page 92 we defined $\mathcal{T}_{small}$ to be the set of conjugacy classes of simple transitive subgroups of S_n of order at most n^5 and in Lemma 7.4.4 we proved that $|\mathcal{T}_{small}| \leq 2n^{4(5\log_2 n+1)}$, so we have

$$|\mathcal{G}_3| \leq 4n^{4(5\log_2 n+1)}.$$

9.5 Large values of n

First we deal with $Pr(E_{imprim})$. Note that E_{imprim} is the same as the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup of S_n. We have specified X in such a way that the pair $g_{\Delta_1}, g_{\Delta_2}$ is not contained in an imprimitive maximal subgroup $S_{n/2} \wr S_2$. Furthermore since 4 does not divide n there is no imprimitive maximal subgroup $S_{n/4} \wr S_4$ of S_n. Define E_{imprim_1} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup $S_{n/3} \wr S_3$ of S_n, and E_{imprim_2} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in an imprimitive maximal subgroup $S_{n/k} \wr S_k$ of S_n, where k is a proper divisor of n such that $k \geq 5$. Then we have

$$E_{imprim} = E_{imprim_1} \cup E_{imprim_2},$$

and consequently

$$Pr(E_{imprim}) \leq Pr(E_{imprim_1}) + Pr(E_{imprim_2}).$$

Lemma 9.5.1. *If $n \geq 150$, then $Pr(E_{imprim_1}) < p/7$.*

Proof. This is proved by an argument identical to that used in the proof of Lemma 8.2.1. □

Lemma 9.5.2. *If $n \geq 226$, then $Pr(E_{imprim_2}) < p/7$.*

Proof. This is proved by an argument identical to that used in the proof of Lemma 8.2.3. □

Now we deal with E_{prim}. For $i \in \{1, 2, 3\}$ define E_{prim_i} to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a primitive maximal subgroup M of A_n such that $M = G \cap A_n$, and $M \in G_i$, that is G is in part i of Theorem 9.4.1. Then since $n \equiv 2 \pmod 4$, by Theorem 9.4.1

$$E_{prim} = E_{prim_1} \cup E_{prim_2} \cup E_{prim_3},$$

and consequently

$$Pr(E_{prim}) \leq Pr(E_{prim_1}) + Pr(E_{prim_2}) + Pr(E_{prim_3}).$$

Lemma 9.5.3. *If $n \geq 46$, and $i \in \{1, 2\}$ then $Pr(E_{prim_i}) < p/7$.*

Proof. We apply Lemma 8.2.2 with $\mathcal{M} = \mathcal{G}_i$, and then use an argument identical to that in the proof of Lemma 8.2.4. □

Lemma 9.5.4. *If* $n \geq 522$*, then* $Pr(E_{prim_3}) < p\,/7$*.*

Proof. We apply Lemma 8.2.2 with $\mathcal{M} = \mathcal{G}_3$, and then use an argument identical to that in the proof of Lemma 8.2.5. □

At this point we have sufficient information to conclude that if $n \geq 522$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$.

If M is a maximal subgroup of A_n, then $M = G \cap A_n$ for a subgroup G such that $G = N_{S_n}(\operatorname{soc} G)$ (note that it may or may not be the case that $N_{S_n}(\operatorname{soc} G) < A_n$.) The next lemma is similar to Lemma 8.2.6 and refers to the cohorts of primitive groups described in [7].

Lemma 9.5.5. *The number of conjugacy classes of primitive subgroups G of S_n such that $G = N_{S_n}(\operatorname{soc} G)$ is bounded above by the number of cohorts of primitive groups of degree n.*

Proof. Let $[G]_{S_n}$ be a conjugacy class of primitive subgroups of S_n such that $G = N_{S_n}(\operatorname{soc} G)$. Then $[\operatorname{soc} G]_{S_n}$ is a corresponding conjugacy class of subgroups, which is represented by exactly one cohort, of degree n. Moreover, $[G]_{S_n}$ is the only conjugacy class of primitive maximal subgroups which corresponds to this cohort. Thus we have established an injection from the set of conjugacy classes of primitive subgroups G of S_n such that $G = N_{S_n}(\operatorname{soc} G)$ into the set of cohorts of primitive groups of degree n. □

For $n \leq 1000$, we see in [7, Table B.4] that there are at most 10 cohorts of primitive groups which act with degree n, excluding the alternating and affine group. Since each conjugacy class $[G]_{S_n}$ of subgroups of S_n corresponds directly to either one or two conjugacy classes $[G \cap A_n]_{A_n}$ of subgroups of A_n, we may apply Lemma 8.2.2 with $\mathsf{M} = 22$.

Lemma 9.5.6. *If* $34 \leq n \leq 1000$*, then* $Pr(E_{prim}) < 5p/7$.

Proof. This is proved by an argument identical to that used in the proof of Lemma 8.2.7. □

We summarise our results. Recall that $n \equiv 2 \pmod 4$.

If ...	then ...
$n \geq 148$	$Pr(E_{imprim_1}) < p/7$
$n \geq 226$	$Pr(E_{imprim_2}) < p/7$
$n \geq 46$	$Pr(E_{prim_i}) < p/7$ for $i \in \{1,2\}$
$n \geq 522$	$Pr(E_{prim_3}) < p/7$
$34 \leq n \leq 1000$	$Pr(E_{prim}) < 5p/7$

Table 9.3: Summary of results in Section 9.5

Proof of Theorem 1.1.1 part 3 for $n \geq 226$. As remarked earlier, we have

$$Pr(E_{imprim}) \leq Pr(E_{imprim_1}) + Pr(E_{imprim_2}),$$

$$Pr(E_{prim}) \leq Pr(E_{prim_1}) + Pr(E_{prim_2}) + Pr(E_{prim_3}),$$

and

$$Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim}).$$

Using the results given in the table above, we conclude that if $n \geq 226$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$. Our result follows. □

9.6 Medium values of n

By Lemma 9.5.6 we know that if $34 \leq n \leq 1000$, then $Pr(E_{prim}) < 5p/7$. It remains to show that $Pr(E_{imprim}) < 2p/7$.

Lemma 9.6.1. *If* $30 \leq n \leq 222$*, then* $Pr(E_{imprim}) < 2p/7$.

Proof. This proof is similar to the proof of Lemma 8.3.1. We use two `GAP` programs and apply the theory on imprimitive maximal subgroups developed in Chapter 6.

The first program, with filename `countingpartitions` and included as Appendix B, is explained and used in the proof of Lemma 8.3.1.

The second program, with filename `medium_an`, is included as Appendix G. This is the `GAP` program `medium` used in the proof of Lemma 8.3.1 with the following modifications. We test values of n such that $n \equiv 2 \pmod 4$. We consider only odd values of $|\Delta_1|$ and $|\Delta_2|$, such that $1 \leq |\Delta_1|, |\Delta_2| \leq n/2$ to take account of how we have now defined our set I. Furthermore, if $|\Delta_1| = |\Delta_2| = n/2$, then again from the definition of I, we have $i \geq 1$, and so in this case we calculate the variable `combprob` for the variable `i` taking values in the list `[1..n/2-1]`.

Before we run the program `medium_an`, we must define a variable `test`, which must be a list of integers containing the values of n which we which to consider. As in `medium`, a value of n is added to a list `bad_n` if we consider it and fail to prove that $Pr(E_{imprim})$ is sufficiently small.

This proof therefore is achieved by the following sequence of commands and output in `GAP`:

```
gap>Read("c:/gap4r4/countpartitions");
gap>test:=[6..224];
>[6..224]
gap>Read("c:/gap4r4/medium_an");
gap>bad_n;
>[6,10,14,18,22,26]
```
□

Proof of Theorem 1.1.1 part 3 for $34 \leq n \leq 222$. By Lemmas 9.5.6 and 9.6.1, we have that if $34 \leq n \leq 222$, then $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$. Our result follows. □

9.7 Small values of n

Our result does not follow for values of n less than 34 because the bound for $Pr(E_{prim})$ is too high. In the next lemma, for the small values of n, we use the GAP data library to provide the orders of primitive maximal subgroups, and thus obtain a tighter upper bound for $Pr(E_{prim})$.

First, the following short GAP program tells us that if $n \equiv 2 \pmod 4$ and $n \leq 30$, then S_n has two conjugacy classes of primitive maximal subgroups, namely A_n and one other, and A_n has only one conjugacy class of primitive maximal subgroups, and these subgroups are $G \cap A_n$, where G is a primitive maximal subgroup of S_n other than A_n.

```
gap>for n in [6,10,14,18,22,26,30] do Print("\n",n);
>   ms:=MaximalSubgroupClassReps(SymmetricGroup(n));
>   for g in ms do if IsPrimitive(g,[1..n]) then Print(g);fi;od;
>   ma:=MaximalSubgroupClassReps(AlternatingGroup(n));
>   for g in ma do if IsPrimitive(g,[1..n]) then Print(g);fi;od;
>od;
```

The output of this code is the following.

```
>6 AlternatingGroup(6) PGL(2,5) PSL(2,5)
10 AlternatingGroup(10) P\Gamma L(2,9) M(10)
14 AlternatingGroup(14) PGL(2,13) PSL(2,13)
18 AlternatingGroup(18) PGL(2,17) PSL(2,17)
22 AlternatingGroup(22) M(22):2 M(22)
26 AlternatingGroup(6) P\GammaL(2,25) P\Sigma L(2,25)
30 AlternatingGroup(6) PGL(2,29) PSL(2,29)
```

This means that for these $n \leq 30$, the event E_{prim} is the same as event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a primitive maximal subgroup of S_n other than A_n.

Lemma 9.7.1. *If $n \in \{26, 30\}$, then $\mu(A_n) = 2^{n-2}$.*

Proof. This proof uses two GAP programs. The first is called countpartitions, and was used and discussed in the proof of Lemma 9.6.1. The second is called small_an and is included as Appendix H. Before running the program small_an, we must define a variable called test, which must be a list of integers containing the values of n which we wish to consider. The first part of small_an is identical to the first part of program medium_an which was used in Lemma 9.6.1, and it calculates an upper bound for $Pr(E_{imprim})$ using the theory developed in Chapter 6. This bound is assigned to the variable ub_imprim.

The second part of small_an calculates an upper bound for $Pr(E_{prim})$ in the same way as the second part of the program small. By Lemmas 5.2.2 and 5.2.4,

$$Pr(E_{prim}) < \frac{n^2|M|}{(n/2-1)!^2},$$

where M is a primitive maximal subgroup of S_n other than A_n. The program small_an calculates the upper bound for $Pr(E_{prim})$ given in this inequality, and assigns it to the variable ub_prim.

Recall that $Pr(E_{\{\Delta_1,\Delta_2\}}) \leq Pr(E_{imprim}) + Pr(E_{prim})$, and we aim to show that $Pr(E_{\{\Delta_1,\Delta_2\}}) < p$ where $p = 1/e2^n$. We have an upper bound ub_imprim+ub_prim for $Pr(E_{\{\Delta_1,\Delta_2\}})$, and in the final part of small_an we compare this bound to p. If it exceeds p, that is, if our bound fails to be sufficiently low, we add the value of n under consideration to the list bad_n.

This proof therefore is completed by the following sequence of commands and output in GAP:

```
gap>Read("c:/gap4r4/countpartitions"); test:=[6..30];;
gap>Read("c:/gap4r4/small_an"); bad_n;
>[ 6,10,14,18,22].
```

□

9.8 $n = 22$

The upper bound for $Pr(E_{prim})$ obtained in the previous proof is too high to be used in the case $n = 22$, so in Lemma 9.8.2 we calculate an even lower bound. We also increase our target by reducing the degree of our graph Γ. We give a preliminary lemma. Recall the notation $C(\Delta)$ which denotes the set of elements of S_n which have orbits Δ and $\Omega\backslash\Delta$, and let $\mathcal{S}$ be the conjugacy class of maximal subgroups of S_n which are permutation isomorphic to $M(22) : 2$ (acting with degree 22 in the usual way).

Lemma 9.8.1. *S_{22} has only one conjugacy class of primitive maximal subgroups other than A_{22}; it is $\mathcal{S}$ as defined above. Let $H \in \mathcal{S}$.*

1. *The only bi-cycles contained in H are $(11, 11)$-cycles.*

2. *H contains 120 elements which are $(11, 11)$-cycles, from each of 672 different $C(\Delta)$. In total H contains $672 \times 120 = 80\,640$ elements which are $(11, 11)$-cycles.*

Proof. 1. We use a `GAP` program called `s22bicycles` which is included as Appendix I. First, `s22bicycles` puts representatives of the conjugacy classes of primitive maximal subgroups of S_{22} other than A_{22} in a list called `primsubgroups`. Second it determines the cycle lengths of the elements of each of these representatives, and whenever it encounters a bi-cycle, it adds the name of the representative together with the cycle lengths to a set called `bicycles`. This proof is therefore achieved by the following sequence of commands and output in `GAP`:

```
gap>Read("c:/gap4r4/s22subgroups"); primsubgroups;
>[M(22):2].
gap>bicycles;
>[[M(22):2],[11]].
```

2. Again we use the GAP program called `s22bicycles`. The third part of this program assigns the representative of $\mathcal{S}$ to the variable `m11`. It makes a list `11_11cycles` of all the $(11,11)$-cycles in `m11`, and a set `11orbits` of the orbits of length 11 of these bi-cycles. Then for each orbit in `11orbits`, it counts how many of the elements of `11_11cycles` have this as an orbit, and assigns this total to a set called `results`.This proof is therefore achieved by the following sequence of GAP commands and output.

```
gap>Read("c:/gap4r4/s22bicycles"); Length(set11orbits);
>672
gap>results;
>[120].
gap>Length(11_11cycles);
>80640
```

□

Even though this result allows us to calculate a tighter upper bound for $P(E_{prim})$, it is still not low enough to apply the Lovász Local lemma. We solve this problem in our next lemma. Recall that in Section 8.1 we defined a set I of $2^{n-2} = 2^{22-2}$ subsets of $\Omega = \{1, \ldots, 22\}$, a set X of order 2^{22-2} which we hope will be a pairwise generating set for S_{22}, and a graph Γ which has the two element subsets of I as its vertex set. We need to prove that

$$Pr(E_{\{\Delta_1,\Delta_2\}})\, e(d+1) < 1,$$

where d is the degree of Γ. If $n = 22$, then part 1 of Lemma 9.8.1 tells us that only some of the pairs of elements of X can possibly be contained in a maximal subgroup of S_n other than A_n. As a result of this, we can reduce the maximum degree of our graph Γ. Then our bound for $Pr(E_{\{\Delta_1,\Delta_2\}})$ is sufficiently low.

Lemma 9.8.2. $\mu(A_{22}) = 2^{22-2}$.

Proof. Let $n = 22$. The set X contains at most one element from each of the intransitive maximal subgroups of S_{22}. By Lemma 6.3.1, the only elements of X which are contained in imprimitive maximal subgroups of S_{22} are the $(11, 11)$-cycles. By our previous lemma, the only elements of X which are contained in primitive maximal subgroups of S_{22} are the $(11, 11)$-cycles. Recall that

$$I_2 = \{\Delta \subset \Omega : |\Delta| = n/2 \text{ and } 1 \in \Delta\}.$$

It follows that the pair $g_{\Delta_1}, g_{\Delta_2}$ can only be contained in a maximal subgroup if $\{\Delta_1, \Delta_2\} \subset I_2$. Indeed for any vertex v of Γ, the probability $Pr(E_v)$ is non-zero only when $v \subset I_2$. Therefore we may reduce the edge set of Γ so that a pair v, v' of vertices is joined only we have both $v \subset I_2$ and $v' \subset I_2$ (as well as $v \cap v' \neq \emptyset$). The graph Γ retains the property that for each vertex v, the event E_v is independent of the events $\{E_u : u \neq v\}$. However, since

$$|I_2| = \frac{1}{2}\binom{22}{11} = 352\,716,$$

the maximum degree of Γ is now

$$d = 2(|I_2| - 2) = 705\,428.$$

Now we find an upper bound for $Pr(E_{prim})$. From Lemma 5.1.1,

$$\begin{aligned} Pr(E_{prim}) &\leq \sum_{H \in \mathcal{S}} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|} \\ &= \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in \mathcal{S}} |C(\Delta_1) \cap H||C(\Delta_2) \cap H|. \end{aligned}$$

By Lemma 9.8.1, for all $H \in \mathcal{S}$, if $C(\Delta_1) \cap H \neq \emptyset$ then $|C(\Delta_1) \cap H| = 120$, so

$$Pr(E_{prim}) \leq \frac{1}{|C(\Delta_1)||C(\Delta_2)|} \sum_{H \in \mathcal{S}} 120|C(\Delta_2) \cap H|$$

From Lemma 5.2.1 we know that a fixed bi-cycle is contained in at most n^2 conjugates of any subgroup of S_n, so

$$\sum_{H \in \mathcal{S}} |C(\Delta_2) \cap H| \leq n^2 |C(\Delta_2)|.$$

Substituting this, and a lower bound for $|C(\Delta_1)|$ from Lemma 5.2.4, we have

$$\begin{aligned} Pr(E_{prim}) &\leq \frac{120}{|C(\Delta_1)||C(\Delta_2)|} \times n^2|C(\Delta_2)| \\ &= \frac{120n^2}{(n/2-1)!^2}. \end{aligned}$$

Finally, we use the GAP program countpartitions as in previous proofs, and then a program called n22_an, which is included as Appendix J. The first part of n22_an is identical to the first part of the programs medium_an and small_an which were used in Lemmas 9.6.1 and 9.7.1 respectively, and calculates an upper bound for $Pr(E_{imprim})$ using the theory developed in Chapter 6. This bound is assigned to the variable ub_imprim.

The second part of n22_an calculates an upper bound for $Pr(E_{prim})$ using the inequality above, and assigns it to the variable ub_prim. So we have an upper bound ub=ub_imprim+ub_prim for $Pr(E_{\{\Delta_1,\Delta_2\}})$. In the final part of n22_an we check that ub $e(d+1) < 1$, and if not we add this value of n to the list bad_n (of course in this case we have $n = 22$).

We run the following sequence of commands and output in GAP:

```
gap>Read("c:/gap4r4/countpartitions"); test:=[22];
>[22]
gap>Read("c:/gap4r4/n22_an"); bad_n;
>[ ].
```

Therefore ub $e(d+1) < 1$, so $Pr(E_{\{\Delta_1,\Delta_2\}})e(d+1) < 1$. We apply the Lovász Local lemma and conclude that the probability that X generates S_{22} pairwise is non-zero. □

9.9 $n \in \{10, 14, 18\}$

Using GAP, we can show that bi-cycles that have two orbits of odd length and that are contained in transitive maximal subgroups of A_{18} are $(3,15)$-cycles and $(9,9)$-cycles in imprimitive subgroups, and 17-cycles and $(9,9)$-cycles in

PSL(2, 17). It follows that

$$\mu(A_{18}) \geq \binom{18}{5} + \binom{18}{7} = 2^{18-2} - [\binom{18}{1} + \binom{18}{3} + \frac{1}{2}\binom{18}{9}].$$

Using similar arguments we can show that

$$\mu(A_{14}) \geq \binom{14}{3} + \binom{14}{5} = 2^{14-2} - [\binom{14}{1} + \frac{1}{2}\binom{14}{7}],$$

and

$$\mu(A_{10}) \geq \binom{10}{1} + \binom{10}{3} = 2^{10-2} - \frac{1}{2}\binom{10}{5}.$$

However, neither constructive or probabilistic methods have so far yielded a full solution to these cases.

Chapter 10

A question from Maróti

In this chapter we answer in the affirmative a question posed to us recently. We give results of an asymptotic nature, that is, we give a lower bound for $\mu(A_n)$, when n is sufficiently large. These results could be strengthened, or possibly made explicit using the techniques given earlier in this thesis.

10.1 Introduction

Maróti asked the following question:

> Is $\mu(A_n) \geq n^3$ for all but finitely many values of n ?

We answer this question in the affirmative. In fact we prove the following theorem which is a stronger result. This theorem could be strengthened significantly by some refinement of our proofs, and could also be made explicit.

Theorem 10.1.1. *Let n be a positive integer. If n is sufficiently large then:*

1. *If n is prime and not of the form $n = (q^d - 1)/(q - 1)$ where d is an integer such that $d \geq 2$ and q is a prime power, we have*

$$\mu(A_n) \geq (n-2)!\,;$$

2. *If n is prime, we have*

$$\mu(A_n) \geq \lfloor n!/n^3 2^{n-1} \rfloor\,;$$

3. *If n is odd, we have*

$$\mu(A_n) \geq \left\lfloor \frac{2^{\sqrt{n}}}{2^7 n^2 \sqrt{n}} \right\rfloor ;$$

4. *If n is even and $n \equiv 2 \pmod 4$, we have*

$$\mu(A_n) = 2^{n-2};$$

5. *If n is even, we have*

$$\mu(A_n) \geq \binom{n}{n/10}.$$

As in previous chapters, our starting point is to consider a covering for A_n (a minimal covering if one is available), and look for a pairwise generating set which consists of at most one element from each subgroup in this covering.

For odd values of n we look for pairwise generating sets for A_n which consist of n-cycles only (when n is odd, an n-cycle is an even permutation). We consider odd prime values of n in Section 10.2 and odd composite values of n in Section 10.3. For even values of n, in Section 10.4 we look for pairwise generating sets for A_n which consist of $(p, n-p)$-cycles only, where p is a prime such that $n/10 \leq p \leq n/5$ (when n is even, a bi-cycle is an even permutation). Part 4 of this theorem follows from Theorem 1.1.1. We give constructive proofs for odd prime values of n, and probabilistic proofs for composite values of n.

10.2 n is prime

We will prove that when n is prime and $n \neq 11, 23$ there are only three types of maximal subgroups of S_n other than A_n, and only three types of maximal subgroups of A_n. We first state a theorem of Guralnick.

Theorem 10.2.1. *[9, Theorem 1] Let G be a nonabelian simple group with $H < G$ and $|G : H| = p^a$, p prime. One of the following holds:*

1. *$G = A_n$ and $H \cong A_{n-1}$ with $n = p^a$;*

2. *$G = \mathrm{PSL}(d,q)$ and H is the stabilizer of a line or hyperplane. Then $|G : H| = (q^d - 1)/(q - 1) = p^a$ (note d must be prime and $d > 2$);*

3. *$G = \mathrm{PSL}(2,11)$ and $H \cong A_5$;*

4. *$G = M_{23}$ and $H \cong M_{22}$ or $G = M_{11}$ and $H \cong M_{10}$;*

5. *$G = \mathrm{PSU}(4,2) \cong \mathrm{PSp}(4,3)$ and H is the parabolic subgroup of index 27.*

Now we use Guralnick's theorem together with the O'Nan-Scott theorem.

Theorem 10.2.2. *Let p be a prime integer, and let M be a maximal subgroup of S_p other than A_p. If $p \neq 11, 23$, then M is one of the following:*

1. Intransitive, *$S_k \times S_{p-k}$, $1 \leq k < p/2$;*

2. Affine, *$\mathrm{AGL}(1,p)$;*

3. Linear almost simple, *$N_{S_p}(\mathrm{PSL}(d,q))$, $p = (q^d - 1)/(q - 1)$ for an integer $d \geq 2$ and prime power q.*

If M is a maximal subgroup of A_p, then $M = G \cap A_p$ where G is one of the above.

Proof. Let M be a maximal subgroup of S_p other than A_p. Because p is prime, S_p does not have imprimitive maximal subgroups, so if M is transitive then it is primitive, and by the O'Nan-Scott theorem (see Theorem 2.1.3) it is a wreath (product action), affine, diagonal or almost simple. However M is not a wreath (product action) because p is not a proper power of a prime, and M is not diagonal because p is not a power of an order of a finite simple group (the order of any finite simple group is even, and we rule out $p = 2$ because S_2 does not have any maximal subgroups). If M is almost simple, then $\operatorname{soc} M$ is a non-abelian finite simple group which acts transitively with degree p and so has a non-trivial subgroup of index p (a point stabiliser). Then we apply Theorem 10.2.1 and we observe that the only possibility is that $\operatorname{soc} M = \mathrm{PSL}(d,q)$ where $p = (q^d - 1)/(q - 1)$. □

Let $n = p > 2$ be an odd prime integer. The subgroups $M \cap A_p$, where M is $\mathrm{AGL}(1,p)$ or M is $S_k \times S_{p-k}$, where $1 \leq k < \lfloor p/3 \rfloor$ is a covering for A_p: the p-cycles are contained in the affine maximal subgroups; A_p does not contain bicycles; and an element of A_p which is a union of at least three disjoint cycles is contained in at least one of the intransitive maximal subgroups in this covering. The order of this covering, and hence an upper bound for $\mu(A_p)$, is

$$(p-2)! + \sum_{1 \leq k < \lfloor p/3 \rfloor} \binom{p}{k}.$$

If p is not of the form $p = (q^d - 1)/(q - 1)$ for an integer $d \geq 2$ and prime power q, then it is straightforward to find a pairwise generating set for A_p of order $(p-2)!$ which consists of one p-cycle from each affine maximal subgroup, as we see in the proof of Theorem 10.1.1 part 1 below.

The Sylow-p subgroups of S_p are cyclic groups of order p, each consisting of $p - 1$ elements which are p-cycles together with the identity element. Each distinct pair of Sylow-p subgroups intersect trivially, and there are $(p-1)!$ elements which are p-cycles in S_p. Therefore there are $(p-2)!$ Sylow-p subgroups of S_p which disjointly contain all the p-cycles.

The abstract group $\mathrm{AGL}(1,p)$ is the group of affine transformations of a vector space of dimension 1 over a field of order p. These affine transformations are bijections, so $\mathrm{AGL}(1,p)$ acts with degree p and the images of the permutation representations of this action is the conjugacy class of affine maximal subgroups of S_p. It is a semi-direct product, that is $\mathrm{AGL}(1,p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$, and is the union of a cyclic subgroup of order p and p conjugate cyclic subgroups of order $p - 1$. Each pair of these subgroups of $\mathrm{AGL}(1,p)$ intersect trivially, and $|\mathrm{AGL}(1,p)| = p(p-1)$. Since the subgroups of S_p which are permutation isomorphic to $\mathrm{AGL}(1,p)$ are maximal, there are $(p-2)!$ such subgroups. The cyclic subgroup of order p of an affine maximal subgroup is a Sylow-p subgroup of S_p. It follows that a Sylow-p subgroup is contained in exactly one affine maximal subgroup, since there are an equal number of each.

Proof of Theorem 10.1.1 part 1. Let p not be of the form $p = (q^d - 1)/(q - 1)$ for an integer $d \geq 2$ and prime power q, and let $p \neq 11, 23$. Let the set X consist of exactly one p-cycle from each Sylow-p subgroup of S_p, so $|X| = (p-2)!$ and $X \subset A_p$. A p-cycle is transitive on Ω, so the elements of X are not contained in intransitive maximal subgroups. Since each affine maximal subgroup contains exactly one Sylow-p subgroup, each affine maximal subgroup contains exactly one element of X. By Theorem 10.2.2 there are no further maximal subgroups of A_p. Therefore no pair of elements of X is contained in a maximal subgroup of A_p, so X generates A_p pairwise. □

When p is of the form $p = (q^d - 1)/(q - 1)$ for an integer $d \geq 2$ and prime power q, we find a pairwise generating set for A_p which consists of at most one p-cycle from each affine maximal subgroup, but we must also take into account the linear almost simple primitive maximal subgroups of A_p. We give a preliminary lemma prior to the proof of Theorem 10.1.1 part 2.

Lemma 10.2.3. *Let p be a prime integer such that $p \geq 25$ and $p = (q^d - 1)/(q-1)$ for an integer $d \geq 2$ and prime power q, and let $P = N_{S_p}(\mathrm{PSL}(d, q))$ be a linear almost simple primitive subgroup of S_p. Then P contains less than*

$$2^{p-1}/(p-1)$$

Sylow-p subgroups of S_p.

Proof. We count pairs (H, K) in two ways, where H is a Sylow-p subgroup of S_p, and K is conjugate to P in S_p and K contains H. Let r be the number of such pairs.

First we have $r = xy$, where x is the number of Sylow-p subgroups of S_p, and y is the number of subgroups of S_p which are conjugate to P and which contain a fixed Sylow-p subgroup of S_p. The number y is the same for all fixed Sylow-p subgroups because they are all conjugate in S_p. Then $x = (p-2)!$ and by Lemma 5.2.1 we have $y < p$. Therefore $r < p(p-2)!$.

Second we have $r = zw$, where z is the number of Sylow-p subgroups of S_p contained in a fixed subgroup conjugate to P, and w is the number of subgroups which are conjugate to P. Now P is primitive, so by [17, Corollary 1.4] is of order less than 2^{p-1}. Then since $P = N_{S_p}(\mathrm{PSL}(d, q))$, by the Orbit-Stabilizer theorem there are more than $p!/2^{p-1}$ such subgroups, so $w > p!/2^{p-1}$. Therefore $r > zp!/2^{p-1}$.

Comparing these two bounds for r gives $p(p-2)! > zp!/2^{p-1}$, so $z < 2^{p-1}/(p-1)$. □

Proof of Theorem 10.1.1 part 2. Let $p \geq 25$ and let p be of the form $p = (q^d - 1)/(q - 1)$ for an integer $d \geq 2$ and prime power q. We do not rule out the possibility that there may be more than one pair q, d such that $p = (q^d - 1)/(q - 1)$. However since $(q^d - 1)/(q - 1) = q^{d-1} + \ldots + q + 1$, it follows that $2 \leq q < p$ and d is determined by q, so there are certainly less than p such pairs. Therefore there are less than p conjugacy classes of maximal linear almost simple primitive subgroups of S_p. We describe an iterative process to find a set X of p-cycles which consists of at most one p-cycle from each Sylow-p subgroup of S_p such that no pair is contained in a maximal linear almost simple primitive subgroup of S_p. Then by Theorem 10.2.2, no pair of elements of X is contained in a maximal subgroup of A_p, so X generates A_p pairwise.

Define $\mathcal{S}_1$ to be the conjugacy class of Sylow-p subgroups of S_p, so $|\mathcal{S}_1| = (p-2)!$. For $2 \leq q < p$, if an integer d exists such that $p = (q^d - 1)/(q - 1)$, and if $N_{S_p}(\mathrm{PSL}(d, q))$ is a primitive maximal subgroup of either A_p or S_p, define $\mathcal{L}_{q_1}$ to be the conjugacy class of subgroups of S_p which are permutation isomorphic to $N_{S_p}(\mathrm{PSL}(d, q))$. For the remainder of this proof we ignore those q for which no such d exists, or for which $N_{S_p}(\mathrm{PSL}(d, q))$ is not a primitive maximal subgroup of A_p or S_p. If $H \in \mathcal{L}_{q_1}$, then $H = N_{S_p}(H)$ is a primitive group acting with degree $p \geq 25$ so $|N_{S_p}(H)| < 2^{p-1}$ by [17, Corollary 1.4]. Then by the Orbit-Stabilizer theorem, $|\mathcal{L}_{q_1}| > p!/2^{p-1}$.

Let $x_1 \in S_p$ be a p-cycle. For each q, let L_{q_1} be the set of subgroups in $\mathcal{L}_{q_1}$ which contain x_1. Then $|L_{q_1}| < p$ by Lemma 5.2.1. Let S_1 be the set of Sylow-p subgroups which are contained in all of the subgroups in all of the L_{q_1}. Since there are less than p different L_{q_1}, each containing less than p subgroups, each of which by Lemma 10.2.3 contain at most $2^{p-1}/(p-1)$ Sylow-p subgroups, it follows that

$$|S_1| < p^2 2^{p-1}/(p-1).$$

Let $\mathcal{S}_2 = \mathcal{S}_1 \setminus S_1$, so $\mathcal{S}_2$ is the set of Sylow-p subgroups of S_p, none of which are contained in the same linear almost simple subgroup as the element x_1. Now $|\mathcal{S}_2| > (p-2)! - p^2 2^{p-1}/(p-1)$, so $|\mathcal{S}_2| > 0$. Let x_2 be any p-cycle from any of the subgroups in $\mathcal{S}_2$, and let $X_2 = \{x_1, x_2\}$. Then X_2 is a set of order 2 which generates A_p pairwise. We continue in the same manner, using the following method for the i-th iteration:

> If $|\mathcal{S}_i| > 0$, let x_i be any p-cycle from any of the subgroups in $\mathcal{S}_i$, and let $X_i = X_{i-1} \cup \{x_i\}$. For each q, let L_{q_i} be the set of subgroups in $\mathcal{L}_{q_i}$ which contain x_i, and let S_i be the set of Sylow-p subgroups which are contained in all of the subgroups in all of the L_{q_i}. Then $|S_i| < p^2 2^{p-1}/(p-1)$. Let $\mathcal{S}_{i+1} = \mathcal{S}_i \setminus S_i$, so $|\mathcal{S}_{i+1}| > (p-2)! - ip^2 2^{p-1}/(p-1)$.

This can be repeated until $\mathcal{S}_{i+1} = \emptyset$ for some value of i. Then the set X_i is a set of order i that generates S_p pairwise. Since $|\mathcal{S}_{i+1}| > (p-2)! - ip^2 2^{p-1}/(p-1)$, we have $|\mathcal{S}_{i+1}| > 0$ if $(p-2)! - ip^2 2^{p-1}/(p-1) > 0$, that is if $i < (p-1)!/p^2 2^{p-1} = p!/p^3 2^{p-1}$. Therefore $X = X_{\lfloor p!/p^3 2^{p-1} \rfloor}$ is a pairwise generating set for A_p of order $\lfloor p!/p^3 2^{p-1} \rfloor$. □

10.3 n is odd composite

When n is not prime there are more types of maximal subgroup of A_n to consider, and we return to the probabilistic method of previous chapters.

Let n be an odd composite number and suppose that p is the smallest non-trivial divisor of n. The subgroups $M \cap A_n$, where M is $S_{n/p} \wr S_p$ or M is $S_k \times S_{n-k}$, where $1 \leq k < \lfloor n/3 \rfloor$ is a covering for A_n: the n-cycles are contained in the imprimitive maximal subgroups; A_n does not contain bi-cycles; and an element of A_n which is a union of at least three disjoint cycles is contained in at least one of the intransitive maximal subgroups in this cover. The order of this covering, and so an upper bound for $\mu(A_n)$, is

$$\frac{n!}{(n/p)!^p p!} + \sum_{1 \leq k < \lfloor n/3 \rfloor} \binom{n}{k}.$$

For a fixed divisor k of n, a fixed n-cycle g is contained in exactly one subgroup $S_{n/k} \wr S_k$; the blocks of the subgroup are the orbits of g^k on Ω. We try to find a pairwise generating set X which consists of at most one n-cycle from each subgroup $S_{n/p} \wr S_p$. However, it is possible that some other transitive maximal subgroup of A_n (that is, one not included in this covering) contains a pair of elements of X. As in previous chapters, we find an upper bound for the probability that this is the case, and then if possible, apply the Lovász Local lemma to prove that such a set X exists which does generate A_n pairwise. First we give five preliminary lemmas.

Lemma 10.3.1. *If k is a non-trivial divisor of a positive integer n such that $k < \sqrt{n}$, then we have*

$$|S_{n/k} \wr S_k| > |S_k \wr S_{n/k}|.$$

If k and l are non-trivial divisors of n such that $k < l \leq \sqrt{n}$, then we have

$$|S_{n/k} \wr S_k| > |S_{n/l} \wr S_l|.$$

Proof. Let $A = k!^{k+1}[(n/k)(n/k-1)\dots(k+1)]$. Then

$$\begin{aligned} |S_{n/k} \wr S_k| &= (n/k)!^k k! \\ &= [(n/k)(n/k-1)\dots(k+1)]^k k!^k k! \\ &= A\,[(n/k)(n/k-1)\dots(k+1)]^{k-1}, \end{aligned}$$

and

$$\begin{aligned}|S_k \wr S_{n/k}| &= k!^{n/k}(n/k)! \\ &= k!^k k!^{n/k-k} k![(n/k)(n/k-1)\dots(k+1)] \\ &= A\,k!^{n/k-k}.\end{aligned}$$

Thus

$$\frac{|S_{n/k} \wr S_k|}{|S_k \wr S_{n/k}|} = \frac{[(n/k)(n/k-1)\dots(k+1)]^{k-1}}{k!^{n/k-k}}.$$

This ratio has $(n/k-k)(k-1)$ terms in both the numerator and the denominator (we ignore those terms which are equal to 1). Since $k < \sqrt{n}$, all of the terms in the numerator are greater than k, and all the terms in the denominator are at most k, so the ratio is certainly greater than 1. Therefore $|S_{n/k} \wr S_k| > |S_k \wr S_{n/k}|$.

Now let $B = (n/l)!^k k!$, and note that $k < l \leq \sqrt{n} \leq n/l < n/k$. Then

$$\begin{aligned}|S_{n/k} \wr S_k| &= (n/k)!^k k! \\ &= [(n/k)(n/k-1)\dots(n/l+1)]^k (n/l)!^k k! \\ &= B[(n/k)(n/k-1)\dots(n/l+1)]^k,\end{aligned}$$

and

$$\begin{aligned}|S_{n/l} \wr S_l| &= (n/l)!^l l! \\ &= (n/l)!^{l-k}(n/l)!^k[l(l-1)\dots(k+1)]k! \\ &= B(n/l)!^{l-k}[l(l-1)\dots(k+1)].\end{aligned}$$

Thus

$$\frac{|S_{n/k} \wr S_k|}{|S_{n/l} \wr S_l|} = \frac{[(n/k)(n/k-1)\dots(n/l+1)]^k}{(n/l)!^{l-k}[l(l-1)\dots(k+1)]}.$$

This ratio has $n(l-k)/l$ terms in both the numerator and the denominator (we ignore those terms which are equal to 1). All of the terms in the numerator are greater than n/l, and all the terms in the denominator are at most n/l, so the ratio is certainly greater than 1. Therefore $|S_{n/k} \wr S_k| > |S_{n/l} \wr S_l|$. □

From this Lemma we know that $\max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k|$ is $|S_p \wr S_{n/p}|$ or $|S_{n/k_0} \wr S_{k_0}|$, where p is the smallest divisor of n and k_0 is the second smallest divisor of n. We give an example of a value of n for each of these cases, to show that indeed both do occur.

Example 10.3.1. Let $n = 578 = 2 \cdot 17^2$, then $p = 2$, $k_0 = 17$ and $|S_p \wr S_{n/p} = S_2 \wr S_{289}| = 2!^{289} 289! > |S_{n/k_0} \wr S_{k_0} = S_{34} \wr S_{17}| = 34!^{17} 17!$.

Let $n = 338 = 2 \cdot 13^2$, then $p = 2$, $k_0 = 13$ and $|S_p \wr S_{n/p} = S_2 \wr S_{169}| = 2!^{169} 169! < |S_{n/k_0} \wr S_{k_0} = S_{26} \wr S_{13}| = 26!^{13} 13!$.

However, when n is odd, and sufficiently large, we have the following.

Lemma 10.3.2. *Let n be an odd integer which is the product of at least three primes (not necessarily all distinct), let p be the smallest divisor of n and let k_0 be the second smallest divisor of n. Then if n is sufficiently large we have*

$$\max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k| = |S_{n/k_0} \wr S_{k_0}|.$$

Proof. The result holds trivially if $n = p^3$, since then $k_0 = p^2$ which is the only non-trivial divisor of n other than p. So suppose that $n \neq p^3$, and note that in this case $k_0 \leq \sqrt{n}$. By Lemma 2.2.2 we have

$$\begin{aligned}
|S_{n/k} \wr S_k| &= (n/k)!^k\, k! \\
&> \exp\left[(\tfrac{n}{k} \ln \tfrac{n}{k} - \tfrac{n}{k} + \tfrac{1}{2} \ln \tfrac{n}{k} + \tfrac{1}{2})k + (k \ln k - k + \tfrac{1}{2} \ln k + \tfrac{1}{2})\right] \\
&= \exp[(n \ln n - n \ln k - n + \tfrac{k}{2} \ln n - \tfrac{k}{2} \ln k + \tfrac{k}{2}) \\
&\qquad\qquad\qquad + (k \ln k - k + \tfrac{1}{2} \ln k + \tfrac{1}{2})] \\
&= \exp\left[(n \ln n - n + \tfrac{1}{2}) - n \ln k + (\tfrac{k}{2} + \tfrac{1}{2}) \ln k + (\tfrac{1}{2} \ln n - \tfrac{1}{2})k\right] \\
&> \exp\left[n \ln n - n + \tfrac{1}{2} - n \ln k - \tfrac{1}{2}k\right].
\end{aligned}$$

Since $k_0 \leq \sqrt{n}$, we have $\ln k_0 \leq \frac{1}{2} \ln n$, and

$$\begin{aligned}
|S_{n/k_0} \wr S_{k_0}| &> \exp\left[\tfrac{n}{2} \ln n - n - \tfrac{1}{2}\sqrt{n}\right] \\
&= \exp\left[\tfrac{n}{2} \ln n - O(n)\right].
\end{aligned}$$

Also by Lemma 2.2.2 we have

$$\begin{aligned}|S_p \wr S_{n/p}| &= p!^{n/p}\,(n/p)! \\ &< \exp\left[(p\ln p - p + \tfrac{1}{2}\ln p + 2)\tfrac{n}{p} + (\tfrac{n}{p}\ln n - \tfrac{n}{p}\ln p - \tfrac{n}{p} + \tfrac{1}{2}\ln n - \tfrac{1}{2}\ln p + 2)\right] \\ &= \exp[(1-\tfrac{1}{2p})n\ln p + \tfrac{n}{p}\ln p + (\tfrac{1}{p}-1)n + \tfrac{1}{2}\ln n - \tfrac{1}{2}\ln p + 2]) \\ &< \exp\left[(1-\tfrac{1}{2p})n\ln p + \tfrac{n}{p}\ln n + \tfrac{1}{2}\ln n + 2\right].\end{aligned}$$

We first consider the cases $p = 3$ and $p = 5$. We have

$$\begin{aligned}|S_3 \wr S_{n/3}| &< \exp\left[(1-\tfrac{1}{6})n\ln 3 + \tfrac{n}{3}\ln n + \tfrac{1}{2}\ln n + 2\right] \\ &= \exp\left[\tfrac{n}{3}\ln n + O(n)\right],\end{aligned}$$

and

$$\begin{aligned}|S_5 \wr S_{n/5}| &< \exp\left[(1-\tfrac{1}{10})n\ln 5 + \tfrac{n}{5}\ln n + \tfrac{1}{2}\ln n + 2\right] \\ &= \exp\left[\tfrac{n}{5}\ln n + O(n)\right].\end{aligned}$$

So if $p = 3$ or $p = 5$ we have $|S_{n/k_0} \wr S_{k_0}| > |S_p \wr S_{n/p}|$, and our result holds.

Now note that $p \le n^{\frac{1}{3}}$ so $\ln p \le \frac{1}{3}\ln n$, and suppose that $p \ge 7$. Then

$$\begin{aligned}(1-\tfrac{1}{2p})n\ln p + \tfrac{n}{p}\ln n &\le \tfrac{1}{3}(1-\tfrac{1}{2p})n\ln n + \tfrac{n}{p}\ln n \\ &\le [\tfrac{1}{3}(1-\tfrac{1}{2p}) + \tfrac{1}{p}]n\ln n \\ &\le \tfrac{19}{42}n\ln n.\end{aligned}$$

Substituting this we have

$$\begin{aligned}|S_p \wr S_{n/p}| &< \exp\left[\tfrac{19}{42}n\ln n + \tfrac{1}{2}\ln n + 2\right] \\ &= \exp\left[\tfrac{19}{42}n\ln n + O(n)\right],\end{aligned}$$

and again, our result holds. □

Lemma 10.3.3. *Let n be an odd integer which is the product of at least three primes (not necessarily distinct). Then if n is sufficiently large we have*

$$\frac{|S_{n/p} \wr S_p|}{|S_{n/k} \wr S_k|} \ge 2^{\sqrt{n}-3},$$

where p is the smallest divisor of n and k is any other non-trivial divisor of n.

Proof. By Lemma 10.3.1 we have

$$\max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k| = |S_{n/k_0} \wr S_{k_0}|,$$

where k_0 is the second smallest divisor of n. First suppose that $n \neq p^3$, and note that $p < k_0 \leq \sqrt{n} \leq n/k_0 < n/p$, and $k_0 - p \geq 2$. Let $D = (n/k_0)!^p p!$. Then

$$|S_{n/p} \wr S_p| = D\,[(n/p) \ldots (n/k_0 + 1)]^p,$$

and

$$|S_{k_0} \wr S_{n/k_0}| = D\,(n/k_0)!^{k_0 - p}[k_0 \ldots (p+1)],$$

so if k is any other non-trivial divisor of n,

$$\frac{|S_{n/p} \wr S_p|}{|S_{n/k} \wr S_k|} \geq \frac{[(n/p) \ldots (n/k_0 + 1)]^p}{(n/k_0)!^{k_0 - p}[k_0 \ldots (p+1)]}.$$

This ratio has $n(k_0 - p)/k_0$ terms in both the numerator and the denominator (ignoring those terms which are equal to 1). All of the terms in the numerator are greater than n/k_0, and all of the terms in the denominator are at most n/k_0, so the ratio is certainly greater than 1. Furthermore, the number of terms in the denominator which are less than $n/2k_0$ is at least $(n/2k_0 - 1/2 - 1)(k_0 - p) \geq \sqrt{n} - 3$ (there are this many in the factor $(n/k_0)!^{k_0-p}$, and perhaps more in the factor $[k_0 \ldots (p+1)]$.) Therefore the ratio is at least $[(n/k_0)/(n/2k_0)]^{\sqrt{n}-3} = 2^{\sqrt{n}-3}$.

Now suppose that $n = p^3$, so in this case $k = p^2$. Then

$$\frac{|S_{n/p} \wr S_p|}{|S_{n/k} \wr S_k|} = \frac{|S_{p^2} \wr S_p|}{|S_p \wr S_{p^2}|} = \frac{p^2!^p\, p!}{p!^{p^2}\, p^2!} = \frac{[p^2 \ldots (p+1)]^{p-1}}{p!^{p^2-p}}.$$

(We have cancelled $p^2!\,p!^p$). This ratio has $(p^2 - p)(p-1)$ terms in both the numerator and the denominator (ignoring those terms which are equal to 1). All of the terms in the denominator are at most p. All of the terms in the numerator are greater than p, and at least $(p-1)(p^2 - 2p + 1) = (p-1)^3$ of these terms are at least $2p$. Therefore the ratio is at least $2^{(p-1)^3}$ which is greater that $2^{\sqrt{n}-3}$ when n is sufficiently large. □

Lemma 10.3.4. *Let n be a positive integer, and let Π be the set of blocks for an imprimitive maximal subgroup H of S_n which is $S_{n/k} \wr S_k$, where k is a non-trivial divisor of n. Let $C(\Pi)$ be the set of n-cycles in H. Then*

$$|C(\Pi)| = \frac{|S_{n/k} \wr S_k|}{n}.$$

Proof. We show that for a fixed n-cycle g and a fixed divisor k of n, the set of orbits of g^k on Ω is the unique set of k blocks for g. We write $g = (\omega_1 \dots \omega_n)$ so then

$$g^k = (\omega_1 \omega_{k+1} \dots \omega_{n-k+1})(\omega_2 \omega_{k+2} \dots \omega_{n-k+2}) \dots (\omega_k \omega_{2k} \dots \omega_n).$$

For $1 \leq i \leq k$, let $\mathcal{O}_i$ be the orbit $\{\omega_{i+jk} : 0 \leq j < n/k\}$ of g^k on Ω. Then $\mathcal{O}_i^{g^j} = \mathcal{O}_{i+j \pmod k}$, so $\{\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k\}$ is a set of k blocks for g.

Conversely, in a set of k blocks for g, suppose that B is the block that contains ω_1. Since g is an n-cycle, it acts transitively on the set of blocks. Therefore $B, B^g, \dots, B^{g^{k-1}}$ are all distinct, and the set of blocks must be $\{B, B^g, \dots, B^{g^{k-1}}\}$. We have $\omega_2 = \omega_1^g \in B^g, \dots, \omega_k = \omega_1^{g^{k-1}} \in B^{g^{k-1}}$, and it follows that $\{\omega_{i+jk} : 0 \leq j < n/k\} = B^{g^{i-1}}$ for $1 \leq i \leq k$. That is a set of k blocks for g is the set of orbits of g^k on Ω.

So the n-cycles in H are precisely those n-cycles g for which the orbits of g^k on Ω are the blocks for H. We count the number of such n-cycles $g = (\omega_1 \dots \omega_n)$. We may assume that $\omega_1 = 1$ and so the block containing ω_1 is the orbit of g^k containing 1, we label this block B_1. Then ω_2 may be an element of any of the $k-1$ remaining blocks - we choose which block and label it B_2. Then ω_3 be an element of any of the remaining $k-2$ blocks - we choose which block and label it B_3. Continuing in this manner we have $(k-1)!$ choices until we have determined which block corresponds to which orbit. Then there are different possibilities for the order in which the elements of each block appear in the n-cycle g, as we now explain. The element $\omega_1 = 1$ is fixed, but ω_2 can be any of the n/k elements from B_2. Continuing in this manner, for all i such that $2 \leq i \leq k$, the element ω_i can be any of the n/k elements from B_i, thus we have $(n/k)^{k-1}$ choices. Then ω_{k+1} can be any of the $n/k-1$ remaining elements from $B_1 \setminus \omega_1$, and for all i such that $1 \leq i \leq k$, the element ω_{k+i} can be any of the $n/k-1$ remaining elements from $B_i \setminus \omega_i$, so we have a further $(n/k-1)^k$ choices. Similarly ω_{2k+i} can be any of the $n/k-2$ remaining elements from $B_i \setminus \{\omega_i, \omega_{k+i}\}$. Continuing in this manner we have a further $(n/k-2)^k \ldots 2^k 1^k$ choices until all the ω_i are determined. Thus the total number of n-cycles in H is

$$(k-1)!\,(n/k)^{k-1}(n/k-1)^k(n/k-2)^k \ldots 2^k 1^k = k!\,(n/k)!^k/n.$$

□

The proof of Lemma 10.3.4 uses mostly counting arguments, but we now give an outline of two more group theoretical proofs in addition.

For a fixed non-trivial divisor k of n, each n-cycle is contained in exactly one imprimitive maximal subgroup $S_{n/k} \wr S_k$ (suppose g is the n-cycle, then it is contained in the subgroup for which the system of blocks is set of orbits of g^k on Ω). Since these subgroups are conjugate in S_n, there are the same number of n-cycles in each one, so all the n-cycles in S_n are divided equally between them. Using the orbit-stabiliser theorem and maximality of $S_{n/k} \wr S_k$ in S_n, there are $n!/|S_{n/k} \wr S_k|$ imprimitive maximal subgroups $S_{n/k} \wr S_k$ in S_n. The number of n-cycles in S_n is $(n-1)!$, so each $S_{n/k} \wr S_k$ contains $(n-1)!\,/\,(n!/|S_{n/k} \wr S_k|) = |S_{n/k} \wr S_k|/n$.

Alternatively, we will show that the set of n-cycles in a fixed $S_{n/k} \wr S_k$ is a single conjugacy class. Then since the group stabiliser of an n-cycle is simply the cyclic group generated by the n-cycle itself, by the orbit-stabiliser theorem we have $|C(\Pi)|\,|\mathbb{Z}_n| = |S_{n/k} \wr S_k|$. Suppose that $g = (\omega_1 \ldots \omega_n)$ and $g' = (\omega'_1 \ldots \omega'_n)$ are contained in the same $S_{n/k} \wr S_k$. Then the orbits of g^k on Ω (namely $\{\omega_{i+jk} : 0 \leq j < n/k\}$ for $1 \leq i \leq k$) are the same as the orbits of g'^k on Ω (namely $\{\omega'_{i+jk} : 0 \leq j < n/k\}$ for $1 \leq i \leq k$), and they are the blocks for this subgroup. Let h be the permutation which maps $\omega_i \mapsto \omega'_i$ for $1 \leq i \leq n$. Then $g^h = g'$, and h is also in the same $S_{n/k} \wr S_k$, since for $1 \leq i \leq k$, we have $\{\omega_{i+jk} : 0 \leq j < n/k\}^h = \{\omega'_{i+jk} : 0 \leq j < n/k\}$, that is h preserves the block system for the subgroup.

Lemma 10.3.5. *Let $n = pq$ where p and q are distinct prime integers. Let Π be a partition of Ω into p subsets of order q, and let $C(\Pi)$ be set of n-cycles in S_n which are elements of the imprimitive maximal subset of S_n which is $S_q \wr S_p$ and for which Π is the set of blocks.*

1. *There are $q!^{p-1}$ imprimitive maximal subgroups H of S_n which are permutation isomorphic to $S_p \wr S_q$ and such that $C(\Pi) \cap H \neq \emptyset$.*

2. *If H is an imprimitive maximal subgroup H of S_n which is $S_p \wr S_q$, and if $C(\Pi) \cap H \neq \emptyset$, then $|C(\Pi) \cap H| = (p-1)!(q-1)!$.*

Proof. 1. We write $\Pi = \{B_1, \ldots, B_p\}$ and first we show that imprimitive maximal subgroups H of S_n which are permutation isomorphic to $S_p \wr S_q$ and such that $C(\Pi) \cap H \neq \emptyset$, are precisely those subgroups for which the set of blocks $\Phi = \{C_1, \ldots, C_q\}$ has the property

$$|B_i \cap C_j| = 1 \text{ for all } 1 \leq i \leq p \text{ and } 1 \leq j \leq q.$$

Then we show that there are $q!^{p-1}$ candidates for Φ.

First let H be an imprimitive maximal subgroup of S_n having a set of blocks $\Phi = \{C_1, \ldots, C_q\}$ satisfying the property above. For each pair i, j such that $1 \leq i \leq p$ and $1 \leq j \leq q$, let $\omega_{i+(j-1)p}$ be the (unique) element of $B_i \cap C_j$, and let $g = (\omega_1 \ldots \omega_n)$. Then $B_i = \{\omega_{i+(l-1)p} : 1 \leq l \leq q\}$, so $B_i^g = \{\omega_{(i+1)+(l-1)p \pmod n} : 1 \leq l \leq q\} = B_{i+1 \pmod p}$, so Π is a set of blocks for g. By a similar argument, Φ is also a set of blocks for g. Therefore $g \in C(\Pi) \cap H$, and so $C(\Pi) \cap H \neq \emptyset$.

Now let $C(\Pi) \cap H \neq \emptyset$, where H is $S_p \wr S_q$, and $\Phi = \{C_1, \ldots, C_q\}$ is the set of blocks for H. Let $g = (\omega_1 \ldots \omega_n) \in C(\Pi) \cap H$. Then Π is the set of orbits of

g^p on Ω, and Φ is the set of orbits of g^q on Ω, and for $1 \leq i \leq p$, $1 \leq j \leq q$, we may assume that B_i is the block containing ω_i and C_j is the block containing ω_j. Then $B_i = \{\omega_{i+(l-1)p} : 1 \leq l \leq q\}$ and $C_j = \{\omega_{j+(l-1)q} : 1 \leq l \leq p\}$, so $B_i \cap C_j = \{\omega_m : 1 \leq m \leq n \text{ and } m \equiv i \pmod p \text{ and } m \equiv j \pmod q\}$. Then $|B_i \cap C_j| = 1$ by the Chinese remainder theorem.

Now we count the candidates for partitions $\Phi = \{C_1, \ldots, C_q\}$ of Ω into subsets of order p satisfying the property above. Suppose that $B_1 = \{\omega_1, \ldots, \omega_q\}$, and for $1 \leq j \leq q$ let C_j be the subset containing ω_j. Then since C_1 contains exactly one element from each B_i, there are q^{p-1} choices for the other $p-1$ elements of C_1. Similarly C_2 contains exactly one element from each $B_i \setminus (B_i \cap C_1)$, there are $(q-1)^{p-1}$ choices for the other $p-1$ elements of C_2. Continuing in this manner we make $q!^{p-1}$ choices in order to determine all the elements of the C_j, so there are this many candidates for Φ.

2. Suppose that H is an imprimitive maximal subgroup H of S_n which is $S_p \wr S_q$, and let $g = (\omega_1 \ldots \omega_n) \in C(\Pi) \cap H$. We show that there are $(p-1)!(q-1)!$ possible candidates for g.

The orbits of g^p on Ω are the sets in Π, and the orbits of g^q on Ω are the blocks for H. Suppose without loss of generality that $\omega_1 = 1$. Let $B_1 \in \Pi$ be the set containing ω_1 and let C_1 be the block for H containing ω_1. Then ω_2 may be an element of any of the $p-1$ remaining sets of $\Pi \setminus B_1$ and any of the $q-1$ remaining blocks of $\Phi \setminus C_1$. Continuing in this manner, there are a total of $(p-1)!(q-1)!$ choices until the order in which the elements $\omega_1, \ldots, \omega_q$ appear in the blocks of Π and Φ is determined. There are no further choices, since $|B_i \cap C_j| = 1$ for all i and j, by the proof of part 1. Moreover any g determined in this manner is contained in $C(\Pi) \cap H$, so the number of such g is $(p-1)!(q-1)!$. □

We now give outline of an alternative proof for part 2. of Lemma 10.3.5.

Let n, p, g and $C(\Pi)$ be as defined in Lemma 10.3.5, and suppose that H and H' are imprimitive maximal subgroups of S_n that are which are permutation isomorphic to $S_p \wr S_q$ and such that $C(\Pi) \cap H \neq \emptyset$ and $C(\Pi) \cap H' \neq \emptyset$. Let $\Phi = \{C_1, \ldots, C_q\}$ and $\Phi' = \{C'_1, \ldots, C'_q\}$ be the sets of blocks for H and H' respectively, and let g be the permutation defined by $g : B_i \cap C_j \mapsto B_i \cap C'_j$ for $1 \leq i \leq p$, $1 \leq j \leq q$. Then $(C(\Pi) \cap H)^g = C(\Pi) \cap H'$, so $|C(\Pi) \cap H| = |C(\Pi) \cap H'|$. Therefore by Lemma 10.3.4. and Lemma 10.3.5 part 1, we have $|C(\Pi) \cap H| = |C(\Pi)|/q!^{p-1} = (p-1)!(q-1)!$.

Proof of Theorem 10.1.1 part 3. Let n be an odd composite integer, and let p be the smallest (prime) non-trivial divisor of n. Define

$$I' = \{\Pi : \Pi \text{ is a partition of } \Omega \text{ into } p \text{ subsets of order } n/p\}.$$

Then $|I'| = \frac{n!}{(n/p)!^p p!}$. Let I be a non-empty subset of I'. For each $\Pi \in I$, let $C(\Pi)$ be the set of n-cycles g such that Π is the set of orbits of g^p, and choose $g_\Pi \in C(\Pi)$ uniformly and independently at random. Define

$$X = \{g_\Pi : \Pi \in I\},$$

so we have $|X| = |I|$. We aim to show that the probability that X generates A_n pairwise is non-zero if $|X| < \frac{2^{\sqrt{n}}}{2^7 n^2 \sqrt{n}}$.

Define a graph $\Gamma = (V, E)$ as follows. The vertices of Γ are the two element subsets of I. For example for each pair $\Pi_1, \Pi_2 \in I$ such that $\Pi_1 \neq \Pi_2$, we have a vertex $\{\Pi_1, \Pi_2\}$. A pair v, v' of vertices are joined by an edge precisely when $v \cap v' \neq \emptyset$. Therefore

$$|V| = \binom{|I|}{2} = \binom{|X|}{2},$$

and each vertex has degree d, where

$$d = 2(|I| - 2) = 2(|X| - 2).$$

Let $v = \{\Pi_1, \Pi_2\}$ be a vertex of Γ. We consider the probability that the corresponding pair of elements g_{Π_1}, g_{Π_2} of X generates a proper subgroup of

A_n. Define E_v to be the event that the pair g_{Π_1}, g_{Π_2} is contained in a maximal subgroup of A_n. Define E_{imprim} to be the event that the pair g_{Π_1}, g_{Π_2} is contained in an imprimitive maximal subgroup of A_n, and define E_{prim} to be the event that the pair g_{Π_1}, g_{Π_2} is contained in a primitive maximal subgroup of A_n.

If the pair g_{Π_1}, g_{Π_2} is contained in a maximal subgroup of A_n, it is transitive because g_{Π_1} and g_{Π_2} are n-cycles. Therefore

$$E_v = E_{imprim} \cup E_{prim},$$

and consequently

$$Pr(E_v) \leq Pr(E_{imprim}) + Pr(E_{prim}).$$

First we consider $Pr(E_{imprim})$. The imprimitive maximal subgroups of A_n are $M \cap A_n$, where M is an imprimitive maximal subgroup of S_n. Note that no pair of elements of X is contained in a subgroup $S_{n/p} \wr S_p$. If $n = p^2$, then these are the only imprimitive maximal subgroups of S_n, so $Pr(E_{imprim}) = 0$. Suppose that n is the product of at least three primes (not necessarily all distinct). We have

$$\begin{aligned}
Pr(E_{imprim}) &\leq \sum_{\substack{k|n \\ k\neq 1,p,n}} \sum_{H\in[S_{n/k}\wr S_k]} \frac{|C(\Pi_1)\cap H|}{|C(\Pi_1)|}\frac{|C(\Pi_2)\cap H|}{|C(\Pi_2)|} \\
&\leq \sum_{\substack{k|n \\ k\neq 1,p,n}} \sum_{H\in[S_{n/k}\wr S_k]} \frac{|H|}{|C(\Pi_1)|}\frac{|C(\Pi_2)\cap H|}{|C(\Pi_2)|} \\
&\leq \frac{1}{|C(\Pi_1)|} \max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k}\wr S_k| \sum_{\substack{k|n \\ k\neq 1,p,n}} \sum_{H\in[S_{n/k}\wr S_k]} \frac{|C(\Pi_2)\cap H|}{|C(\Pi_2)|}.
\end{aligned}$$

From Lemma 5.2.1 we know that a fixed n-cycle is contained in less than n conjugates of any subgroup of S_n, so

$$\sum_{H\in[S_{n/k}\wr S_k]} |C(\Pi_2)\cap H| < n|C(\Pi_2)|.$$

Substituting this we have

$$
\begin{aligned}
Pr(E_{imprim}) &< \frac{1}{|C(\Pi_1)|} \max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k| \sum_{\substack{k|n \\ k\neq 1,p,n}} n \\
&< \frac{n\sqrt{n}}{|C(\Pi_1)|} \max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k| \\
&= \frac{n^2\sqrt{n}}{|S_{n/p} \wr S_p|} \max_{\substack{k|n \\ k\neq 1,p,n}} |S_{n/k} \wr S_k|
\end{aligned}
$$

(this last substitution follows from Lemma 10.3.4). Using the result from Lemma 10.3.3, if n is sufficiently large then

$$
\begin{aligned}
Pr(E_{imprim}) &< \frac{2^3 n^2 \sqrt{n}}{2^{\sqrt{n}}} \\
&= \exp[-n^{1/2} \ln 2 + \frac{5}{2} \ln n + 3 \ln 2].
\end{aligned}
$$

Now suppose that $n = pq$, where p and q are distinct primes. We have

$$
Pr(E_{imprim}) \leq \sum_{H \in [S_p \wr S_q]} \frac{|C(\Pi_1) \cap H|}{|C(\Pi_1)|} \frac{|C(\Pi_2) \cap H|}{|C(\Pi_2)|}.
$$

By Lemma 10.3.5, the number of terms in this sum is certainly at most $q!^{p-1}$, and the same lemma gives values for $|C(\Pi_1) \cap H|$ and $|C(\Pi_2) \cap H|$. Thus

$$
\begin{aligned}
Pr(E_{imprim}) &\leq q!^{p-1} \frac{[(p-1)!(q-1)!]^2}{|C(\Pi_1)||C(\Pi_2)|} \\
&= q!^{p-1} \left[\frac{(p-1)!(q-1)!n}{q!^p p!} \right]^2 \\
&= \frac{1}{q!^{p-1}}.
\end{aligned}
$$

We examine the reciprocal of this last expression, and we use the lower bound for a factorial given in Lemma 2.2.2.

$$
\begin{aligned}
q!^{p-1} &\geq \exp \left[(p-1) \left(q \ln q - q + \frac{1}{2} \ln q + \frac{1}{2} \right) \right] \\
&= \exp \left[\frac{p}{2} (q \ln q - q) \right] \\
&= \exp \left[\frac{n}{2} \ln q - \frac{n}{2} \right] \\
&> \exp \left[\frac{n}{4} \ln n - \frac{n}{2} \right].
\end{aligned}
$$

(This last line follows because $q > \sqrt{n}$.) We conclude that if $n = pq$, where p and q are distinct primes, and if n is sufficiently large then we have

$$Pr(E_{imprim}) < \exp\left[-\frac{n}{4}\ln n + \frac{n}{2}\right].$$

Now we consider $Pr(E_{prim})$. Let $M_1, \ldots, M_r$ be a complete set of representatives of the conjugacy classes of primitive maximal subgroups of A_n. Then

$$\begin{aligned} Pr(E_{prim}) &\leq \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|C(\Pi_1) \cap H|}{|C(\Pi_1)|} \frac{|C(\Pi_2) \cap H|}{|C(\Pi_2)|} \\ &\leq \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|H|}{|C(\Pi_1)|} \frac{|C(\Pi_2) \cap H|}{|C(\Pi_2)|} \\ &\leq \frac{1}{|C(\Pi_1)|} 2^{n-1} \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|C(\Pi_2) \cap H|}{|C(\Pi_2)|} \\ &\leq \frac{1}{|C(\Pi_1)|} 2^{n-1} \sum_{i=1}^{r} n. \end{aligned}$$

From [15] we know that the number of primitive (not necessarily maximal) subgroups of S_n is bounded above by $n^{c_1 \ln n}$, so $2n^{c_1 \ln n}$ certainly provides an upper bound for the number of primitive maximal subgroups of A_n. So we have $r \leq 2n^{c_1 \ln n}$, and we substitute $|C(\Pi_1)|$ from Lemma 10.3.4. So

$$\begin{aligned} Pr(E_{prim}) &< \frac{n}{(n/p)!^p p!} 2^{n-1} 2n^{1+c_1 \ln n} \\ &= \frac{n^{2+c_1 \ln n} 2^n}{(n/p)!^p p!}, \end{aligned}$$

when n is sufficiently large. We use the lower bound for factorials given in

Lemma 2.2.2 again to see that

$$\begin{aligned}
(n/p)!^p p! &> \exp\left[p\left(\frac{n}{p}\ln n - \frac{n}{p}\ln p - \frac{n}{p} + \frac{1}{2}\ln n - \frac{1}{2}\ln p + \frac{1}{2}\right)\right. \\
&\qquad\qquad \left. + \left(p\ln p - p + \frac{1}{2}\ln p + \frac{1}{2}\right)\right] \\
&= \exp\left[n\ln n - n\ln p - n + \frac{p}{2}\ln n + \frac{p}{2}\ln p - \frac{p}{2} + \frac{1}{2}\ln p + \frac{1}{2}\right] \\
&> \exp\left[n\ln n - n\ln p - n - \frac{p}{2}\right] \\
&> \exp\left[\frac{n}{2}\ln n - n - \frac{\sqrt{n}}{2}\right].
\end{aligned}$$

Therefore if n is sufficiently large,

$$\begin{aligned}
Pr(E_{prim}) &< \exp\left[2\ln n + n\ln 2 + c_1\ln^2 n - \frac{n}{2}\ln n + n + \frac{\sqrt{n}}{2}\right] \\
&= \exp\left[-\frac{n}{2}\ln n + (1+\ln 2)n + \frac{\sqrt{n}}{2} + c_1\ln^2 n\right].
\end{aligned}$$

Comparing our upper bounds for $Pr(E_{imprim})$ and $Pr(E_{prim})$, we see that if n is sufficiently large, then the largest of these is $\frac{2^3n^2\sqrt{n}}{2^{\sqrt{n}}}$, that is the upper bound for $Pr(E_{imprim})$ when n is a product of three or more primes. Then since $Pr(E_v) \leq Pr(E_{imprim}) + Pr(E_{prim})$, we have

$$Pr(E_v) < \frac{2^4n^2\sqrt{n}}{2^{\sqrt{n}}}.$$

Recall that $d = 2|X|-4$ is the degree of our graph Γ. If $Pr(E_v)\,e(d+1) < 1$, then we can apply the Lovász Local lemma (see Lemma 4.3.1) to conclude that $Pr(\bigcap_{v\in V}\overline{E_v}) > 0$. Now if n is sufficiently large, and if

$$|X| \leq \frac{2^{\sqrt{n}}}{2^7n^2\sqrt{n}},$$

then certainly

$$\begin{aligned}
Pr(E_v)\,e(d+1) &= Pr(E_v)\,e(2|X|-3) \\
&< Pr(E_v)2e|X| < 1.
\end{aligned}$$

Since $\bigcap_{v\in V}\overline{E_v}$ is precisely the event that X generates A_n pairwise, we have $\mu(A_n) \geq \lfloor\frac{2^{\sqrt{n}}}{2^7n^2\sqrt{n}}\rfloor$ if n is sufficiently large. □

10.4 n is even

When n is even, the subgroups $M \cap A_n$, where M is $S_{n/2} \wr S_2$ or M is $S_k \times S_{n-k}$, where k is odd and $1 \leq k < n/2$ is a covering for A_n: A_n does not contain n-cycles; the $(n/2, n/2)$-cycles, and any element which is the product of disjoint cycles of even length only, are contained in the imprimitive maximal subgroups in this covering; any other element is contained in at least one of the intransitive maximal subgroups in this covering. By Lemma 2.2.1, the order of this covering, and so an upper bound for $\mu(A_n)$, is

$$\begin{array}{ll} 2^{n-2} & \text{if } n \equiv 2 \pmod 4, \\ 2^{n-2} + \frac{1}{2}\binom{n}{n/2} & \text{if } n \equiv 0 \pmod 4. \end{array}$$

The result $\mu(A_n) = 2^{n-2}$ if n is sufficiently large and $n \equiv 2 \pmod 4$ follows from Theorem 1.1.1, but is included as Theorem 10.1.1 part 4 for completeness. In the proof of Theorem 10.1.1 part 5, we again use the probabilistic method. We first give a theorem which classifies maximal subgroups of A_n, which is an extension of [2, Theorem 3] and its proof.

Theorem 10.4.1. *There exists a constant c, such that for all positive integers n and for each maximal subgroup M of A_n, one of the following holds:*

1. $M = (S_k \times S_{n-k}) \cap A_n$, $1 \leq k < n/2$;
2. $M = (S_{n/k} \wr S_k) \cap A_n$, $k \in \{2, 3, 4\}$;
3. $|M| \leq \left(\frac{n}{5e}\right)^n e^{c \ln n}$.

Proof. If M is imprimitive, then $M = (S_{n/k} \wr S_k) \cap A_n$ (imprimitive action), where k is some proper divisor of n. If $k \geq 5$, then $|S_{n/k} \wr S_k| \leq e^7 5^3 \left(\frac{n}{5e}\right)^n n^{\frac{5}{2}}$ by Lemma 2.2.3. If M is primitive, then $|M| \leq 2^{n-1}$ by [17, Corollary 1.4]. □

Proof of Theorem 10.1.1 part 5. Let n be an even integer such that $n \geq 50$, and let p be a prime integer such that $n/10 \leq p \leq n/5$ (such a prime exists by Bertrand's postulate - see [10, Theorem 418]). Define

$$I = \{\Delta \subset \Omega : |\Delta| = p\}.$$

Then $|I| = \binom{n}{p}$. For each $\Delta \in I$, let $C(\Delta)$ be the set of bi-cycles which have orbits Δ and $\Omega \setminus \Delta$, and choose $g_\Delta \in C(\Delta)$ uniformly and independently at random. Define

$$X = \{g_\Delta : \Delta \in I\}.$$

Then $|X| = |I| = \binom{n}{p} \geq \binom{n}{n/10}$, and we aim to show that the probability that X generates A_n pairwise is non-zero.

Define a graph $\Gamma = (V, E)$ as follows. The vertices of Γ are the two element subsets of I. For example for each pair $\Delta_1, \Delta_2 \in I$ such that $\Delta_1 \neq \Delta_2$, we have a vertex $\{\Delta_1, \Delta_2\}$. A pair v, v' of vertices are joined by an edge precisely when $v \cap v' \neq \emptyset$. Therefore

$$|V| = \binom{|I|}{2} = \binom{|X|}{2},$$

and each vertex has degree d, where

$$d = 2(|I| - 2) = 2(|X| - 2).$$

Let $v = \{\Delta_1, \Delta_2\}$ be a vertex of Γ. We consider the probability that the corresponding pair of elements $g_{\Delta_1}, g_{\Delta_2}$ of X generates a proper subgroup of A_n. Define E_v to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of A_n. Let c be the constant used in Theorem 10.4.1, and define E_1 to be the event that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup of A_n of order at most $\left(\frac{n}{5e}\right)^n e^{c \ln n}$. We show that $E_v = E_1$.

Suppose that the pair $g_{\Delta_1}, g_{\Delta_2}$ is contained in a maximal subgroup M of A_n. We prove that M is in part 3 of Theorem 10.4.1. The bi-cycles g_{Δ_1} and g_{Δ_2} are $(p, n-p)$-cycles where p is prime. An intransitive maximal subgroup of S_n is determined by a partition Ω into two subsets - the parts of the partition are the orbits of the group, and the orbits of any element of the group are contained in these two orbits. Since g_{Δ_1} and g_{Δ_2} each have a different pair of orbits on Ω, M is not intransitive. Suppose M is imprimitive, that is $M = (S_{n/k} \wr S_k) \cap A_n$ for some k. Since p is prime, by Lemma 6.3.1 we have $p = n/k$ (and Δ_1 is one of the blocks of M) or $p = k$ (and Δ_1 contains exactly one element from each of the blocks of M). If $p = n/k$, then $k = n/p \geq 5$ since $p \leq n/5$. If $p = k$, then $k \geq 5$ since $p \geq n/10$ and $n \geq 50$. Then by Lemma 2.2.3 we have $|M| \leq \left(\frac{n}{5e}\right)^n e^{c \ln n}$. If M is primitive, then $|M| \leq 2^{n-1}$ by [17, Corollary 1.4]. Therefore M is in part 3 of Theorem 10.4.1, and we conclude that $E_v \subseteq E_1$.

Clearly $E_1 \subseteq E_v$, therefore $E_v = E_1$ and $Pr(E_v) = Pr(E_1)$. We now prove that $Pr(E_1) = o(2^{-n})$, taking the proof from [2, Lemma 8] (modified since that result applied to odd values of n). Let $M_1, \ldots, M_r$ be a complete set of representatives of the conjugacy classes of transitive maximal subgroups of A_n of order at most $\left(\frac{n}{5e}\right)^n e^{c \ln n}$. Then

$$\begin{aligned} Pr(E_1) &\leq \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|C(\Delta_1) \cap H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|} \\ &\leq \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|H|}{|C(\Delta_1)|} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|} \\ &\leq \frac{1}{|C(\Delta_1)|} \left(\frac{n}{5e}\right)^n e^{c \ln n} \sum_{i=1}^{r} \sum_{H \in [M_i]} \frac{|C(\Delta_2) \cap H|}{|C(\Delta_2)|} \\ &\leq \frac{1}{|C(\Delta_1)|} \left(\frac{n}{5e}\right)^n e^{c \ln n} \sum_{i=1}^{r} n. \end{aligned}$$

From [15] we know that the number of primitive (not necessarily maximal) subgroups of S_n is bounded above by $n^{c_1 \ln n}$, and that the number of imprimitive maximal subgroups of S_n is $n^{o(1)}$. Since a conjugacy class of subgroups of S_n splits into at most two conjugacy classes of subgroups of A_n, we have $r \leq n^{c_2 \ln n}$. We use the result $|C(\Delta_1)| \geq e^2 \left(\frac{n-3}{2e}\right)^{n-1}$ from Lemma 5.2.4. Then

$$\begin{aligned} Pr(E_1) &< \left(\frac{2e}{n-3}\right)^{n-1} \left(\frac{n}{5e}\right)^n e^{c \ln n - 2} n^{1 + c_2 \ln n} \\ &= o(2^{-n}). \end{aligned}$$

So if n is sufficiently large, $Pr(E_v) < 1/e(d+1)$. In that case we apply the Lovász Local lemma (see Lemma 4.3.1) to conclude that $Pr(\bigcap_{v\in V} \overline{E_v}) > 0$. Since $\bigcap_{v\in V} \overline{E_v}$ is precisely the event that X generates A_n pairwise, we have $\mu(A_n) \geq \binom{n}{n/10}$. □

Appendix A

A pairwise generating set for S_9

This is a list of length 73. The elements generate S_9 pairwise. This list is used in the proof of Lemma 3.5.3.

```
y:=[(1,2,3,4,5,6)(7,8,9), (1,2,3,6,5,7)(4,9,8), (1,2,4)(3,5,7,9,6,8),
  (1,2,5,9,8,4)(3,7,6), (1,2,8)(3,6,5,9,4,7), (1,2,9,8,4,7)(3,5,6),
  (1,2,9,3,6,5)(4,7,8), (1,3,2)(4,7,9,8,5,6), (1,3,9,4,8,2)(5,7,6),
  (1,3,7,5,9,6)(2,4,8), (1,3,4)(2,6,9,7,5,8), (1,3,5,7,8,4)(2,6,9),
  (1,3,5,7,4,9)(2,6,8), (1,3,7,9,2,6)(4,8,5), (1,3,2,7,8,6)(4,5,9),
  (1,3,5,8,6,7)(2,9,4), (1,4,5)(2,3,9,8,7,6), (1,4,8,6,7,3)(2,5,9),
  (1,4,7,6,8,9)(2,5,3), (1,4,8)(2,5,7,6,3,9), (1,4,2,6,9,5)(3,8,7),
  (1,4,7)(2,6,5,8,3,9), (1,5,2)(3,6,7,4,9,8), (1,5,3,7,9,2)(4,6,8),
  (1,5,9,3,4,8)(2,6,7), (1,5,6)(2,7,9,4,3,8), (1,5,9,3,6,4)(2,8,7),
  (1,5,2,8,4,7)(3,6,9), (1,5,3)(2,9,4,6,7,8), (1,6,2,3,4,8)(5,9,7),
  (1,6,8)(2,3,7,9,4,5), (1,6,7)(2,3,8,5,4,9), (1,6,9,4,7,3)(2,5,8),
  (1,6,4)(2,5,8,9,7,3), (1,6,2,5,8,4)(3,7,9), (1,6,4,2,7,3)(5,9,8),
  (1,6,5,2,8,3)(4,7,9), (1,6,3)(2,9,5,7,4,8), (1,7,8,9,6,2)(3,5,4),
  (1,7,2)(3,6,9,8,4,5), (1,7,9,6,5,2)(3,8,4), (1,7,3)(2,4,6,5,9,8),
  (1,7,9,8,4,5)(2,6,3), (1,7,5,3,4,6)(2,8,9), (1,8,7,3,5,2)(4,6,9),
  (1,8,9,5,2,3)(4,7,6), (1,8,2,4,7,6)(3,5,9), (1,8,3,6,9,7)(2,4,5),
  (1,8,5)(2,6,4,9,3,7), (1,8,2,7,4,3)(5,9,6), (1,8,4,6,5,9)(2,7,3),
  (1,8,9)(2,7,6,5,3,4), (1,8,5,2,9,6)(3,4,7), (1,8,7)(2,9,5,3,6,4),
  (1,9,7,2,4,3)(5,8,6), (1,9,3)(2,5,8,7,6,4), (1,9,3,6,8,4)(2,5,7),
  (1,9,4,3,7,8)(2,5,6), (1,9,6)(2,7,5,8,4,3), (1,9,5,2,7,8)(3,6,4),
  (1,9,7,5,6,4)(2,8,3), (1,9,7)(2,8,4,3,5,6), (1,2,3,8,4,5)(6,9,7),
  (1,4,5,7,2,6)(3,8,9),
  (1,2,3,4,5,6,7,8),(2,3,4,5,6,7,8,9),(1,4,3,5,6,7,8,9),
  (1,2,4,5,6,7,8,9),(2,1,3,5,6,7,8,9),(2,1,3,4,6,7,8,9),
  (1,2,3,4,5,7,8,9),(2,3,1,4,5,6,9,8),(1,2,3,4,5,6,7,9)];
```

Appendix B

GAP program: countpartitions

This program is used in the proofs of the following lemmas: 8.3.1, 8.4.1, 8.5.2, 9.6.1, 9.7.1, 9.8.2.

```
p:=function(x,y)
   local f1,f2,indexf2,tally,f3,f,f4;
   f1:=x; f2:=y;
   # If y is an integer...
   if IsInt(f2) then
      if f1=0 or f2=0 then
         return 1;
      elif IsInt(f1/f2) then
         return Factorial(f1)/(Factorial(f2)^(f1/f2)*Factorial(f1/f2));
      else
         return 0;
      fi;
   fi;
   # If y is a list...
   if IsList(f2) then
      if f1=0 or Sum(f2)=0 then
         return 1;
      elif f1=Sum(f2) then
         # We create f3, a list of the multiplicity of each non-zero
         #                                integer in the list y.
         f3:=[];
         indexf2:=1;
         for f in f2 do
            if indexf2=1 then
               tally:=1;
            else
               if f=f2[indexf2-1] then
                  tally:=tally+1;
               else
                  if f2[indexf2-1]>0 then
                     Append(f3,[tally]);
                  fi;
                  tally:=1;
               fi;
```

```
            if indexf2=Size(f2) and f>0 then
               Append(f3,[tally]);
            fi;
         fi;
         indexf2:=indexf2+1;
      od;
      # We use f3 to calculate our function.
      f4:=Factorial(f1);
      for f in f2 do
         f4:=f4/Factorial(f);
      od;
      for f in f3 do
         f4:=f4/Factorial(f);
      od;
      return f4;
   else
      return 0;
   fi;
 fi;
end;

op:=function(x,y)
 local g1,g2,g3,g;
 g1:=x; g2:=y;
 # If y is an integer...
 if IsInt(g2) then
   if g2=0 then
      return 1;
   elif IsInt(g1/g2) then
      return Factorial(g1)/(Factorial(g2)^(g1/g2));
   else
      return 0;
   fi;
 fi;
 # If y is a list...
 if IsList(g2) then
   if g1=0 or Sum(g2)=0 then
      return 1;
   elif g1=Sum(g2) then
      g3:=Factorial(g1);
      for g in g2 do
         g3:=g3/Factorial(g);
      od;
      return g3;
   else
      return 0;
   fi;
 fi;
end;
```

Appendix C

GAP program: medium

This program is used in the proof of Lemma 8.3.1.

```
# A variable called "test" which is a list of positive integers must be
# defined before this program is run. The program checks all odd integers n
# in this list.
#---------------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#---------------------------------------------------------------------------
bad_n:=[];
for n in test do
   if IsInt((n-1)/2)=true then
      ub:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..(n-1)/2] do   # d1 is $|\Delta_1|$
         cd1:=Factorial(d1-1)*Factorial(n-d1-1);
         for d2 in [0..d1] do
            cd2:=Factorial(d2-1)*Factorial(n-d2-1);
            if d1=d2 then max_i:=d1-1; else max_i:=Minimum(d1,d2); fi;
            for i in [0..max_i] do
               combprob:=0;
               for k in divisors do
                  d1resp:=0; d2resp:=0; d1dis:=0; d2dis:=0;
                  h1:=0; h2:=0; h3:=0; h4:=0;
                  if IsInt(d1*k/n) then   # d1>0
                     d1resp:=Factorial(n/k)^k*(k/n)^2
                            *Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                  fi;
                  if IsInt(d2*k/n) and d2>0 then
                     d2resp:=Factorial(n/k)^k*(k/n)^2
                            *Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
                  fi;
                  if IsInt(d1/k) then
                     d1dis:=Factorial(k)*Factorial(d1/k)^k
```

```
                 *Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) and d2>0 then
   d2dis:=Factorial(k)*Factorial(d2/k)^k
                 *Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
elif d2=0 then
   d2dis:=Factorial(k)*Factorial(n/k)^k/n;
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n) and d2>0
                                    and IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)*p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k) and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                                 *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n) and d2>0
                                       and i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                                 *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
         Append(rest,[((n-d1-d2)/k)+ipart[r]]);
      od;
      h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                      *op(n+i-d1-d2,rest)/Factorial(m0);
      h4:=h4+h;
   od; # ends the ipart loop
```

```
                    prob4:=h4*d1dis*d2dis/(cd1*cd2);
                    combprob:=combprob+prob4;
                 fi;
              od; # ends the k loop
              Append(imprimprob,[combprob]);
           od; # ends the i loop
        od; # ends the d2 loop
     od; # ends the d1 loop
     ub:=Maximum(imprimprob);
#---------------------------------------------------------------------------
# (GAP does not provide a value for e, so we use a number slightly larger).
     target:=1/((2719/1000)*(2^n));
     if (ub<2*target/7)=false then
        Add(bad_n,n);
     fi;
  fi;
od;
#---------------------------------------------------------------------------
```

Appendix D

GAP program: small

This program is used in the proof of Lemma 8.4.1.

```
# A variable called "test" which is a list of positive integers
# must be defined before this program is run. The program checks
# all odd integers n in this list.
#-------------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#-------------------------------------------------------------------------
bad_n:=[];
for n in test do
   if IsInt((n-1)/2)=true then
      ub:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..(n-1)/2] do   # d1 is $|\Delta_1|$
         cd1:=Factorial(d1-1)*Factorial(n-d1-1);
         for d2 in [0..d1] do
            cd2:=Factorial(d2-1)*Factorial(n-d2-1);
            if d1=d2 then max_i:=d1-1; else max_i:=Minimum(d1,d2); fi;
            for i in [0..max_i] do
               combprob:=0;
               for k in divisors do
                  d1resp:=0;
                  d2resp:=0; d1dis:=0; d2dis:=0;
                  h1:=0; h2:=0; h3:=0; h4:=0;
                  if IsInt(d1*k/n) then   # d1>0
                     d1resp:=Factorial(n/k)^k*(k/n)^2
                            *Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                  fi;
                  if IsInt(d2*k/n) and d2>0 then
                     d2resp:=Factorial(n/k)^k*(k/n)^2
                            *Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
                  fi;
                  if IsInt(d1/k) then
```

```
   d1dis:=Factorial(k)*Factorial(d1/k)^k
                *Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) and d2>0 then
   d2dis:=Factorial(k)*Factorial(d2/k)^k
                *Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
elif d2=0 then
   d2dis:=Factorial(k)*Factorial(n/k)^k/n;
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n) and d2>0 and
                                        IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)*p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k) and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                               *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n) and d2>0
                                       and i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                               *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
         Append(rest,[((n-d1-d2)/k)+ipart[r]]);
      od;
      h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                     *op(n+i-d1-d2,rest)/Factorial(m0);
      h4:=h4+h;
```

```
                  od; # ends the ipart loop
                  prob4:=h4*d1dis*d2dis/(cd1*cd2);
                  combprob:=combprob+prob4;
               fi;
            od; # ends the k loop
            Append(imprimprob,[combprob]);
         od; # ends the i loop
      od; # ends the d2 loop
   od; # ends the d1 loop
   ubimprim:=Maximum(imprimprob);
#---------------------------------------------------------------------------
   prim:=0;
   mscr:=MaximalSubgroupClassReps(SymmetricGroup(n));
   i:=2;
   while (i-1)<Length(mscr) do
      if IsPrimitive(mscr[i],[1..n]) then
          prim:=prim+Order(mscr[i]);
      fi;
      i:=i+1;
   od;
   ubprim:=n^2*prim/(Factorial((n-1)/2)*Factorial((n-3)/2));
   ub:=ubimprim+ubprim;
#---------------------------------------------------------------------------
# We compare ub with target=1/e2^n.
# (GAP does not provide a value for e, so we use a number slightly larger).
   target:=1/((2719/1000)*(2^n));
   if ub>target then
      Add(bad_n,n);
   fi;
  fi;
od;
```

Appendix E

GAP program: s21bicycles

This program is used in the proof of Lemma 8.5.1.

```
w:=[1..21];primsubgroups:=[];bicycles:=[];714cycles:=[];21cycles:=[];
list7orbits:=[];set7orbits:=[];results:=[];
#--------------------------------------------------------------------------
mscr:=MaximalSubgroupClassReps(SymmetricGroup(w));
for m in mscr do
   if IsPrimitive(m,w) then
      Add(primsubgroups,m);
   fi;
od;
Remove(primsubgroups,1);    # Removes A_21 from the list
#--------------------------------------------------------------------------
for m in primsubgroups do
   for c in ConjugacyClasses(m) do
      cl:=CycleLengths(Representative(c),w);
      if (Length(cl)=2 or Length(cl)=1)
         and ([m,AsSet(cl)] in bicycles)=false then
         Add(bicycles,[m,AsSet(cl)]);
      fi;
   od;
od;
#--------------------------------------------------------------------------
pgl:=primsubgroups[3];
for c in ConjugacyClasses(pgl) do
   cl:=CycleLengths(Representative(c),w);
   if Length(cl)=2 then
      Append(714cycles,ShallowCopy(AsList(c)));
   fi;
   if Length(cl)=1 then
      Append(21cycles,ShallowCopy(AsList(c)));
   fi;
od;
#--------------------------------------------------------------------------
for g in 714cycles do
   o:=Orbits(Group(g));
   if Length(o[1])=7 then 7orbit:=AsSet(o[1]);
```

```
      else 7orbit:=AsSet(o[2]);
   fi;
   Add(list7orbits,7orbit);
od;
set7orbits:=AsSet(list7orbits);
#--------------------------------------------------------------------------
for orbit1 in set7orbits do
   tally:=0;
   for orbit2 in list7orbits do
      if orbit2=orbit1 then tally:=tally+1; fi;
   od;
   AddSet(results,tally);
od;
```

Appendix F

GAP program: n21

This program is used in the proof of Lemma 8.5.2.

```
# A variable called "test" which is a list of positive integers
# must be defined before this program is run. The program checks
# all odd integers n in this list.
#---------------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#---------------------------------------------------------------------------
bad_n:=[]; ub_imprim:=0; ub_prim:=0;
for n in test do
      ub:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..(n-1)/2] do
         cd1:=Factorial(d1-1)*Factorial(n-d1-1);
         for d2 in [0..d1] do
            if d2=0 then cd2:=Factorial(n-1); else
               cd2:=Factorial(d2-1)*Factorial(n-d2-1);
            fi;
            if d1=d2 then max_i:=d1-1; else max_i:=Minimum(d1,d2); fi;
            for i in [0..max_i] do
               combprob:=0;
               for k in divisors do
                  d1resp:=0; d2resp:=0; d1dis:=0; d2dis:=0;
                  h1:=0; h2:=0; h3:=0; h4:=0;
                  if IsInt(d1*k/n) then   # d1>0
                     d1resp:=Factorial(n/k)^k*(k/n)^2*
                             Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                  fi;
                  if IsInt(d2*k/n) and d2>0 then
                     d2resp:=Factorial(n/k)^k*(k/n)^2*
                             Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
                  fi;
                  if IsInt(d1/k) then
```

```
   d1dis:=Factorial(k)*Factorial(d1/k)^k*
                 Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) and d2>0 then
   d2dis:=Factorial(k)*Factorial(d2/k)^k*
                 Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
elif d2=0 then
   d2dis:=Factorial(k)*Factorial(n/k)^k/n;
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n) and d2>0 and
                                       IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)*p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k) and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                              *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n) and d2>0 and
                                         i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                              *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
         Append(rest,[((n-d1-d2)/k)+ipart[r]]);
      od;
      h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                    *op(n+i-d1-d2,rest)/Factorial(m0);
      h4:=h4+h;
```

```
                od; # ends the ipart loop
                prob4:=h4*d1dis*d2dis/(cd1*cd2);
                combprob:=combprob+prob4;
             fi;
          od; # ends the k loop
          Append(imprimprob,[combprob]);
       od; # ends the i loop
    od; # ends the d2 loop
  od; # ends the d1 loop
  ub_imprim:=Maximum(imprimprob);
#---------------------------------------------------------------------------
  ub_prim:=112/Factorial(5)/Factorial(13);
#---------------------------------------------------------------------------
  ub:=ub_imprim+ub_prim;
  x:=Binomial(21,0)+Binomial(21,3)+Binomial(21,6)+Binomial(21,9)
                                                      +Binomial(21,7);
  # (GAP does not provide a value for e, so we use a similar number)
  if ub*(2719/1000)*((2*x)-3)>1 then
     Add(bad_n,n);
  fi;
od;
```

Appendix G

GAP program: medium_an

This program is used in the proof of Lemma 9.6.1.

```
# A variable called "test" which is a list of positive integers
# must be defined before this program is run. The program checks
# all n \equiv 2 \pmod{4} in this list.
#------------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#------------------------------------------------------------------------
bad_n:=[];
for n in test do
   if IsInt((n-2)/4)=true then
      ub:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..n/2] do
         if IsOddInt(d1) then
            cd1:=Factorial(d1-1)*Factorial(n-d1-1);
            for d2 in [1..d1] do
               if IsOddInt(d2) then
                  cd2:=Factorial(d2-1)*Factorial(n-d2-1);
                  if d1=d2 then max_i:=d1-1;
                                        else max_i:=Minimum(d1,d2); fi;
                  if d1=d2 and d1=n/2 then min_i:=1; else min_i:=0; fi;
                  for i in [min_i..max_i] do
                     combprob:=0;
                     for k in divisors do
                        d1resp:=0; d2resp:=0; d1dis:=0; d2dis:=0;
                        h1:=0; h2:=0; h3:=0; h4:=0;
                        if IsInt(d1*k/n) then
                           d1resp:=Factorial(n/k)^k*(k/n)^2
                            *Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                        fi;
                        if IsInt(d2*k/n) then
                           d2resp:=Factorial(n/k)^k*(k/n)^2
```

```
    *Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
fi;
if IsInt(d1/k) then
   d1dis:=Factorial(k)*Factorial(d1/k)^k
          *Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) then
   d2dis:=Factorial(k)*Factorial(d2/k)^k
          *Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n)
                           and IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)
                              *p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k) and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                       *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n) and i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                       *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
         Append(rest,[((n-d1-d2)/k)+ipart[r]]);
      od;
      h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                  *op(n+i-d1-d2,rest)/Factorial(m0);
```

```
                           h4:=h4+h;
                        od; # ends the ipart loop
                        prob4:=h4*d1dis*d2dis/(cd1*cd2);
                        combprob:=combprob+prob4;
                     fi;
                  od; # ends the k loop
                  Append(imprimprob,[combprob]);
               od; # ends the i loop
            fi;
         od; # ends the d2 loop
      fi;
   od; # ends the d1 loop
   ub:=Maximum(imprimprob);
#----------------------------------------------------------------------------
   target:=1/((2719/1000)*(2^n));
   if (ub<2*target/7)=false then
      Add(bad_n,n);
   fi;
fi;
od;
```

Appendix H

GAP program: small_an

This program is used in the proof of Lemma 9.7.1.

```
# A variable called "test" which is a list of positive integers
# must be defined before this program is run. The program checks
# all n \equiv 2 \pmod{4} in this list.
#------------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#------------------------------------------------------------------------
bad_n:=[];
for n in test do
   if IsInt((n-2)/4)=true then
      ub:=0; ub_prim:=0;ub_imprim:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..n/2] do
         if IsOddInt(d1) then
            cd1:=Factorial(d1-1)*Factorial(n-d1-1);
            for d2 in [1..d1] do
               if IsOddInt(d2) then
                  cd2:=Factorial(d2-1)*Factorial(n-d2-1);
                  if d1=d2 then max_i:=d1-1;
                  else max_i:=Minimum(d1,d2); fi;
                  if d1=d2 and d1=n/2 then min_i:=1;
                  else min_i:=0; fi;
                  for i in [min_i..max_i] do
                     combprob:=0;
                     for k in divisors do
                        d1resp:=0; d2resp:=0; d1dis:=0; d2dis:=0;
                        h1:=0; h2:=0; h3:=0; h4:=0;
                        if IsInt(d1*k/n) then
                           d1resp:=Factorial(n/k)^k*(k/n)^2
                           *Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                        fi;
                        if IsInt(d2*k/n) then
```

```
   d2resp:=Factorial(n/k)^k*(k/n)^2*
    Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
fi;
if IsInt(d1/k) then
   d1dis:=Factorial(k)*Factorial(d1/k)^k
         *Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) then
   d2dis:=Factorial(k)*Factorial(d2/k)^k
         *Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n)
                          and IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)
                             *p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k)
                             and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                       *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n)
                             and i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                       *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
         Append(rest,[((n-d1-d2)/k)+ipart[r]]);
```

```
                              od;
                              h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                                         *op(n+i-d1-d2,rest)/Factorial(m0);
                              h4:=h4+h;
                           od; # ends the ipart loop
                           prob4:=h4*d1dis*d2dis/(cd1*cd2);
                           combprob:=combprob+prob4;
                        fi;
                     od; # ends the k loop
                     Append(imprimprob,[combprob]);
                  od; # ends the i loop
               fi;
            od; # ends the d2 loop
         fi;
      od; # ends the d1 loop
      ub_imprim:=Maximum(imprimprob);
#---------------------------------------------------------------------------
      prim:=0;
      mscr:=MaximalSubgroupClassReps(SymmetricGroup(n));
      i:=2;
      while (i-1)<Length(mscr) do
         if IsPrimitive(mscr[i],[1..n]) then
             prim:=prim+Order(mscr[i]);
         fi;
         i:=i+1;
      od;
      ub_prim:=n^2*prim/(Factorial(n/2-1))^2;
#----------------------------------------------------------------------------
# We compare ub with target=1/e2^n.
# (GAP does not provide a value for e, so we use a slightly larger number).
      ub:=ub_imprim+ub_prim;
      target:=1/((2719/1000)*(2^n));
      if ub>target then
         Add(bad_n,n);
      fi;
   fi;
od;
```

Appendix I

GAP program: s22bicycles

This program is used in the proof of Lemma 9.8.1.

```
w:=[1..22];primsubgroups:=[];bicycles:=[];11_11cycles:=[];
list11orbits:=[];set11orbits:=[];results:=[];
#--------------------------------------------------------------------------
mscr:=MaximalSubgroupClassReps(SymmetricGroup(w));
for m in mscr do
   if IsPrimitive(m,w) then
      Add(primsubgroups,m);
   fi;
od;
Remove(primsubgroups,1);    # Removes A_22 from the list
#--------------------------------------------------------------------------
for m in primsubgroups do
   for c in ConjugacyClasses(m) do
      cl:=CycleLengths(Representative(c),w);
      if (Length(cl)=2 or Length(cl)=1)
         and ([m,AsSet(cl)] in bicycles)=false then
         Add(bicycles,[m,AsSet(cl)]);
      fi;
   od;
od;
#--------------------------------------------------------------------------
m11:=primsubgroups[1];
for c in ConjugacyClasses(m11) do
   cl:=CycleLengths(Representative(c),w);
   if Length(cl)=2 then
      Append(11_11cycles,ShallowCopy(AsList(c)));
   fi;
od;
#--------------------------------------------------------------------------
for g in 11_11cycles do
   o:=Orbits(Group(g));
   if 1 in o[1] then 11orbit:=AsSet(o[1]);
      else 11orbit:=AsSet(o[2]);
   fi;
   Add(list11orbits,11orbit);
```

```
od;
set11orbits:=AsSet(list11orbits);
#-------------------------------------------------------------------------
for orbit1 in set11orbits do
   tally:=0;
   for orbit2 in list11orbits do
      if orbit2=orbit1 then tally:=tally+1; fi;
   od;
   AddSet(results,tally);
od;
```

Appendix J

GAP program: n22_an

This program is used in the proof of Lemma 9.8.2.

```
# A variable called "test" which is a list of positive integers
# must be defined before this program is run. The program checks
# all n \equiv 2 \pmod{4} in this list.
#-----------------------------------------------------------------------
# First we define a function zeros(y) - which returns the number of zeros
# in the list y
zeros:=function(y) local z1,z2,z; z1:=y; z2:=0; for z in z1 do
      if z=0 then z2:=z2+1; fi; od; return z2; end;
#-----------------------------------------------------------------------
test:=[22]; # REMOVE
bad_n:=[];
for n in test do
   if IsInt((n-2)/4)=true then
      ub:=0; ub_prim:=0;ub_imprim:=0; imprimprob:=[];
      divisors:=ShallowCopy(DivisorsInt(n));
      Remove(divisors); Remove(divisors,1);
      for d1 in [1..n/2] do
         if IsOddInt(d1) then
            cd1:=Factorial(d1-1)*Factorial(n-d1-1);
            for d2 in [1..d1] do
               if IsOddInt(d2) then
                  cd2:=Factorial(d2-1)*Factorial(n-d2-1);
                  if d1=d2 then max_i:=d1-1;
                  else max_i:=Minimum(d1,d2); fi;
                  if d1=d2 and d1=n/2 then min_i:=1;
                  else min_i:=0; fi;
                  for i in [min_i..max_i] do
                     combprob:=0;
                     for k in divisors do
                        d1resp:=0; d2resp:=0; d1dis:=0; d2dis:=0;
                        h1:=0; h2:=0; h3:=0; h4:=0;
                        if IsInt(d1*k/n) then
                           d1resp:=Factorial(n/k)^k*(k/n)^2
                           *Factorial((d1*k/n)-1)*Factorial(k-(d1*k/n)-1);
                        fi;
```

```
if IsInt(d2*k/n) then
   d2resp:=Factorial(n/k)^k*(k/n)^2*
    Factorial((d2*k/n)-1)*Factorial(k-(d2*k/n)-1);
fi;
if IsInt(d1/k) then
   d1dis:=Factorial(k)*Factorial(d1/k)^k
         *Factorial((n/k)-(d1/k))^k*k/(d1*(n-d1));
fi;
if IsInt(d2/k) then
   d2dis:=Factorial(k)*Factorial(d2/k)^k
         *Factorial((n/k)-(d2/k))^k*k/(d2*(n-d2));
fi;
if IsInt(d1*k/n) and IsInt(d2*k/n)
                             and IsInt(i*k/n) then
   h1:=p(i,n/k)*p(d1-i,n/k)*p(d2-i,n/k)
                                *p(n+i-d1-d2,n/k);
   prob1:=h1*d1resp*d2resp/(cd1*cd2);
   combprob:=combprob+prob1;
fi;
if IsInt(d1*k/n) and IsInt(d2/k)
                                and i=d1*d2/n then
   h2:=p(i,d2/k)*op(d1-i,(n-d2)/k)*p(d2-i,d2/k)
                          *op(n+i-d1-d2,(n-d2)/k);
   prob2:=h2*d1resp*d2dis/(cd1*cd2);
   combprob:=combprob+prob2;
fi;
if IsInt(d1/k) and IsInt(d2*k/n)
                                and i=d1*d2/n then
   h3:=p(i,d1/k)*op(d2-i,(n-d1)/k)*p(d1-i,d1/k)
                          *op(n+i-d1-d2,(n-d1)/k);
   prob3:=h3*d1dis*d2resp/(cd1*cd2);
   combprob:=combprob+prob3;
fi;
if IsInt(d1/k) and IsInt(d2/k) then
   m:=Minimum(d1/k,d2/k);
   if i=0 then
      partitions:=[List([1..k],i->0)];
   else
      partitions:=RestrictedPartitions(i,[0..m],k);
   fi;
   for ipart in partitions do
      m0:=zeros(ipart);
      d1part:=[];
      for r in [1..k] do
         Append(d1part,[(d1/k)-ipart[r]]);
      od;
      d2part:=[];
      for r in [1..k] do
         Append(d2part,[(d2/k)-ipart[r]]);
      od;
      rest:=[];
      for r in [1..k] do
```

```
                                 Append(rest,[((n-d1-d2)/k)+ipart[r]]);
                              od;
                              h:=p(i,ipart)*op(d1-i,d1part)*op(d2-i,d2part)
                                         *op(n+i-d1-d2,rest)/Factorial(m0);
                              h4:=h4+h;
                           od; # ends the ipart loop
                           prob4:=h4*d1dis*d2dis/(cd1*cd2);
                           combprob:=combprob+prob4;
                        fi;
                     od; # ends the k loop
                     Append(imprimprob,[combprob]);
                  od; # ends the i loop
               fi;
            od; # ends the d2 loop
         fi;
      od; # ends the d1 loop
      ub_imprim:=Maximum(imprimprob);
#--------------------------------------------------------------------------
      ub_prim:=n^2*120/(Factorial(n/2-1))^2;
#---------------------------------------------------------------------------
# We compare ub with target=1/e2^n.
# (GAP does not provide a value for e, so we use a slightly larger number).
      ub:=ub_imprim+ub_prim;
      x:=Binomial(22,11)/2;
      target:=1/((2719/1000)*(2*x-3));
      if ub>target then
         Add(bad_n,n);
      fi;
   fi;
od;
```

Bibliography

[1] Noga Alon and Joel H. Spencer, *The probabilistic method*, second ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience [John Wiley & Sons], New York, 2000, With an appendix on the life and work of Paul Erdős. MR MR1885388 (2003f:60003)

[2] Simon R. Blackburn, *Sets of permutations that generate the symmetric group pairwise*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1572–1581. MR MR2259081 (2007e:20005)

[3] Peter J. Cameron, Peter M. Neumann, and David N. Teague, *On the degrees of primitive permutation groups*, Math. Z. **180** (1982), no. 2, 141–149. MR MR661693 (83i:20004)

[4] J. H. E. Cohn, *On n-sum groups*, Math. Scand. **75** (1994), no. 1, 44–58. MR MR1308936 (95k:20026)

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. MR MR827219 (88g:20025)

[6] Bruce N. Cooperstein, *Minimal degree for a permutation representation of a classical group*, Israel J. Math. **30** (1978), no. 3, 213–235. MR MR0506701 (58 #22255)

[7] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR MR1409812 (98m:20003)

[8] Walter Feit and John G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR MR0166261 (29 #3538)

[9] Robert M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), no. 2, 304–311. MR MR700286 (84m:20007)

[10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, at the Clarendon Press, 1954, 3rd ed. MR MR0067125 (16,673c)

[11] Wolfgang Kimmerle, Richard Lyons, Robert Sandling, and David N. Teague, *Composition factors from the group ring and Artin's theorem on orders of simple groups*, Proc. London Math. Soc. (3) **60** (1990), no. 1, 89–122. MR MR1023806 (91c:20030)

[12] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990. MR MR1057341 (91g:20001)

[13] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), no. 2, 365–383. MR MR916173 (89b:20008)

[14] Martin W. Liebeck and Jan Saxl, *Maximal subgroups of finite simple groups and their automorphism groups*, Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989) (Providence, RI), Contemp. Math., vol. 131, Amer. Math. Soc., 1992, pp. 243–259. MR MR1175777 (93g:20032)

[15] Martin W. Liebeck and Aner Shalev, *Maximal subgroups of symmetric groups*, J. Combin. Theory Ser. A **75** (1996), no. 2, 341–352. MR MR1401008 (98b:20005)

[16] ———, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), no. 2, 497–520. MR MR1639620 (99h:20004)

[17] Attila Maróti, *On the orders of primitive groups*, J. Algebra **258** (2002), no. 2, 631–640. MR MR1943938 (2003j:20004)

[18] ———, *Covering the symmetric groups with proper subgroups*, J. Combin. Theory Ser. A **110** (2005), no. 1, 97–111. MR MR2128968 (2005m:20009)

[19] E. T. Whittaker and G. N. Watson, *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions*, Fourth edition. Reprinted, Cambridge University Press, New York, 1962. MR MR0178117 (31 #2375)

[20] Robert A. Wilson, *The finite simple groups*, In preparation. Version 077 available on line at `www.maths.qmul.ac.uk`, 2007.